McAfee VirusScan para Windows 95 e Windows 98

Guia do Usuário

Network Associates Brasil

Rua Geraldo Flauzino Gomes 78-cj.51

04575-060 Sao Paulo

Brasil

Network Associates Portugal

Av. de Liberdade, 114

1250 Lisboa

Portugal

COPYRIGHT

CONTRATO DE LICENÇA:

NOTA PARA TODOS OS USUÁRIOS: LEIA COM ATENÇÃO O SEGUINTE CONTRATO LEGAL ("CONTRATO"), QUE ESTABELECE OS TERMOS GERAIS DA LICENÇA PARA O SOFTWARE DA NETWORK ASSOCIATES. PARA OBTER OS TERMOS ESPECÍFICOS DA SUA LICENÇA, CONSULTE OS ARQUIVOS README.1ST E LICENSE.TXT, OU OUTRO DOCUMENTO DE LICENÇA QUE ACOMPANHE O SEU SOFTWARE, EM FORMA DE ARQUIVO DE TEXTO OU COMO PARTE DA EMBALAGEM DO SOFTWARE. SE VOCÊ NÃO CONCORDAR COM TODOS OS TERMOS ESTABELECIDOS ANTERIORMENTE, NÃO INSTALE O SOFTWARE. (SE FOR APLICÁVEL, VOCÊ PODE DEVOLVER O PRODUTO AO LOCAL DE AQUISIÇÃO PARA OBTER UM REEMBOLSO TOTAL.)

1. **Concessão de Licença.** Sujeito a pagamento dos honorários de licença aplicáveis e à aceitação dos termos e condições deste Contrato, a Network Associates lhe concede pelo presente documento o direito não exclusivo e não transferível de usar uma cópia da versão especificada do Software e da documentação que o acompanha (a "Documentação"). Você pode instalar uma cópia do Software em seu computador, estação de trabalho, assistente digital pessoal, pager, "telefone inteligente" ou outro dispositivo eletrônico para o qual se destina o Software (cada um deles, um "Dispositivo Cliente"). Se o Software for licenciado como um conjunto ou fizer parte de um pacote com mais de um produto de Software especificado, esta licença aplica-se a todos os produtos de Software especificados, que estão sujeitos a quaisquer restrições ou períodos de uso especificados individualmente para cada um desses produtos de Software na embalagem ou fatura do produto aplicável.

   a. **Utilização.** O Software é licenciado como um produto único; não pode ser utilizado em mais de um Dispositivo Cliente ou por mais de um usuário de cada vez, exceto conforme estabelecido nesta Seção 1. O Software estará "em uso" em um computador quando for descarregado na memória temporária (i.e., memória de acesso aleatório - random-access memory - ou RAM) ou quando foi instalado na memória permanente (por exemplo, disco rígido, CD-ROM ou outro dispositivo de memória) daquela Dispositivo Cliente. Esta licença o autoriza a fazer uma cópia do Software somente para backup ou para arquivamento, contanto que essa cópia contenha todas as informações relativas à propriedade do software.

   b. **Utilização do Modo de Servidor.** De acordo com o estabelecido na embalagem ou fatura do produto aplicável, você pode instalar e usar o Software em um Dispositivo Cliente ou em um servidor ("Servidor") em um ambiente de rede ou multiusuário ("Utilização do Modo de Servidor") para (i) conectar-se, direta ou indiretamente, com um número que não exceda o máximo de Dispositivos Clientes ou "estações" especificados; ou (ii) distribuir não mais do que o número máximo de agentes (pollers)

especificados para distribuição. Se a embalagem ou fatura do produto aplicável não especificar o número máximo de Dispositivos Clientes ou pollers, esta licença lhe concede uma licença para usar um único produto, sujeita às cláusulas da sub-seção (a), acima. É necessária uma licença individual para cada Dispositivo Cliente ou estação que possa ser conectado ao Software em qualquer momento, mesmo que esses Dispositivos Clientes ou estações não estejam conectados ao Software de forma concorrente, ou estejam usando o Software em qualquer momento determinado.

A utilização de software ou hardware que reduza o número de Dispositivos Clientes ou estações conectadas que usem o Software simultaneamente (por exemplo, o uso de software ou hardware de “multiplexação” ou “pooling”) não reduz o número total de licenças que você deve obter. Especificamente, o número de licenças deve ser igual ao número de entradas distintas para o “front end” do software ou hardware de multiplexação ou “pooling”. Especificamente, o número de licenças deve ser igual ao número de entradas distintas para o “front end” do software ou hardware de multiplexação ou “pooling”. Se o número de Dispositivos Clientes ou estações que podem ser conectados ao Software exceder o número de licenças obtidas, você deve ter um mecanismo razoável que assegure que a utilização do Software não ultrapasse os limites especificados na fatura ou na embalagem do produto Esta licença o autoriza a fazer uma cópia ou efetuar o download da Documentação para cada Dispositivo Cliente ou estação licenciada, desde que cada cópia contenha todas as informações de propriedade da Documentação.

c. **Utilização Múltipla.** Se o Software estiver licenciado para uso múltiplo, de acordo com o especificado na embalagem ou fatura do produto, você poderá fazer, usar e instalar em Dispositivos Clientes quantas cópias adicionais do Software quiser, de acordo com as especificadas nos termos de licença de uso múltiplo. Esta licença o autoriza a fazer uma cópia da Documentação, ou obtê-la por download, para cada cópia do Software de acordo com os termos do uso múltiplo, desde que cada cópia contenha todas as informações de propriedade da Documentação. Você deve ter um mecanismo razoável de controle para assegurar que o número de Dispositivos Clientes nos quais o Software está instalado não ultrapasse o número de licenças adquiridas.

2. **Duração.** Esta licença está em vigor durante o período de tempo especificado na fatura ou na embalagem do produto, ou no README.1ST, LICENSE.TXT ou qualquer outro arquivo de texto que acompanhe o Software e se destine a estabelecer os termos do seu contrato de licença. As instâncias que no Contrato estabelecido neste documento entrarem em conflito com as cláusulas da embalagem ou fatura do produto, os documentos README.1ST e LICENSE.TXT, a fatura do produto, a embalagem ou outro documento de texto se constituirão nos termos da sua concessão de licença para uso do Software. Você ou a Network Associates podem terminar a sua licença antes do período especificado no documento adequado de acordo com os termos estabelecidos anteriormente. Este Contrato e a sua licença cessarão automaticamente se você não cumprir com qualquer uma das limitações ou outros requisitos descritos Ao final deste contrato, você deve destruir todas as cópias do Software e da Documentação. Este contrato pode ser rescindido a qualquer momento, destruindo-se todas as cópias do Software e a Documentação, bem como todas as cópias do Software e da Documentação.

3. **Atualizações**. Durante a vigência da licença, é permitido fazer download de atualizações, revisões ou atualizações de versão do Software quando a Network Associates as publicar em seu sistema quadro de avisos eletrônico, site da web ou através de outros serviços online.

4. **Direitos de Propriedade.** O Software e a Documentação são protegidos pelas leis de direito autoral dos Estados Unidos e pelas cláusulas dos tratados internacionais. A Network Associates possui e detém todos os direitos, titularidade e participações em relação ao Software, incluindo todos os direitos autorais, patentes, direitos sobre segredos comerciais, marcas comerciais e outros diretos de propriedade estabelecidos anteriormente. Você reconhece que a posse, instalação ou uso do Software não lhe transfere qualquer direito à propriedade intelectual do Software e que não adquirirá quaisquer direitos sobre o Software exceto os expressamente estabelecidos neste Contrato. Você concorda que quaisquer cópias do Software e da Documentação deverão conter as mesmas informações relativas à propriedade que aparecem no Software e na Documentação.

5. **Restrições.** Não é permitido alugar, arrendar, emprestar ou revender o Software, ou permitir que terceiros se beneficiem do uso e dos recursos do Software através de compartilhamento de tempo, birô de serviços ou qualquer outro tipo de acordo. Não é permitido transferir qualquer direitos que lhe foi concedido por este Contrato. Não é permitido copiar a documentação que acompanha o Software. Não é permitido utilizar engenharia reversa, descompilar ou desassemblar o Software, exceto se esta restrição for expressamente proibida pelas leis vigentes. Não é permitido modificar ou criar trabalhos derivados com base no Software, no todo ou em parte. Não é permitido copiar o Software, exceto o expressamente permitido na Seção 1 acima. Não é permitido remover quaisquer informações relativas à propriedade ou rótulos do Software. Todos os diretos não expressamente aqui estabelecidos são reservados à Network Associates. A Network Associates se reserva o direito de conduzir auditorias periódicas, antecedidas por comunicação escrita, para verificar o cumprimento dos termos deste Contrato.9

6. **Garantia e Renúncia à Garantia**

   a. **Garantia Limitada.** A Network Associates garante que por um período de trinta (30) dias a partir da data da compra original da mídia (por exemplo, os disquetes) no qual o Software está contido, esta não apresentará defeitos de fabricação.

   b. **Indenização do Cliente.** A responsabilidade da Network Associates e de seus fornecedores será, a critério da Network Associates, (i) devolver o valor pago pela licença, se houver, ou (ii) substituir a mídia defeituosa na qual o Software estiver contido por uma cópia da mídia sem defeitos Você deve devolver a mídia defeituosa à Network Associates por sua conta, com uma cópia de seu recibo Esta garantia limitada é anulada se o defeito tiver sido provocado por um acidente, uso indevido ou má utilização. Qualquer mídia de substituição será garantida pelo período restante da garantia original. Fora dos Estados Unidos da América, essa indenização não está disponível na medida em que a Network Associates está sujeita às restrições das leis e normas que regulam a exportação dos Estados Unidos.

Renúncia à Garantia. Dentro dos limites da legislação em vigor e da garantia limitada aqui estabelecida, O SOFTWARE É FORNECIDO SEM GARANTIAS DE QUALQUER NATUREZA, EXPRESSAS OU IMPLÍCITAS, DA FORMA EM QUE SE ENCONTRA. SEM LIMITAR AS CLÁUSULAS ANTERIORES, VOCÊ ASSUME A RESPONSABILIDADE DA ESCOLHA DO SOFTWARE PARA ATINGIR OS RESULTADOS PRETENDIDOS, E PELA INSTALAÇÃO, USO E RESULTADOS OBTIDOS COM ESTE SOFTWARE. SEM LIMITAR AS CLÁUSULAS ANTERIORES, A NETWORK ASSOCIATES NÃO GARANTE QUE O SOFTWARE ESTEJA LIVRE DE ERROS, INTERRUPÇÕES OU OUTROS TIPOS DE FALHAS, OU QUE O SOFTWARE ATENDERÁ ÀS SUAS NECESSIDADES. DENTRO DOS LIMITES DA LEGISLAÇÃO EM VIGOR, A NETWORK ASSOCIATES NEGA TODAS AS GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO MAS NÃO LIMITANDO-SE A GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM DETERMINADO OBJETIVO E À NÃO VIOLAÇÃO DE DIREITOS EM RELAÇÃO AO SOFTWARE E À DOCUMENTAÇÃO QUE O ACOMPANHA. ALGUNS PAÍSES E JURISDIÇÕES NÃO PERMITEM LIMITAÇÕES EM GARANTIAS IMPLÍCITAS, POR ISSO AS LIMITAÇÕES ACIMA PODEM NÃO SE APLICAR A VOCÊ. As cláusulas anteriores serão aplicadas dentro dos limites máximos permitidos pela legislação em vigor.

A compra ou pagamento do Software pode lhe dar direito a garantia adicionais, que a Network Associates especificará na embalagem ou fatura que você irá receber ao adquirir o produto ou no README.1ST , LICENSE.TXT ou outro arquivo de texto que acompanhe o Software e estabeleça os termos de seu contrato de licença. Nos casos em que as cláusulas deste Contrato entrem em conflito com as cláusulas da embalagem ou fatura do produto, o README.1ST, LICENSE.TXT ou documentos semelhantes, a fatura, embalagem ou arquivo de texto estabelecerá os termos de seus direitos de garantia para o Software.

7. **Limitação de Responsabilidade.** EM NENHUMA CIRCUNSTÂNCIA, SEM QUALQUER PRETEXTO LEGAL, SEJA ATO ILÍCITO, CONTRATO OU QUALQUER OUTRA CIRCUNSTÂNCIA, A NETWORK ASSOCIATES OU SEUS FORNECEDORES PODEM SE RESPONSABILIZAR POR VOCÊ OU POR QUALQUER OUTRA PESSOA EM CONSEQÜÊNCIA DE QUALQUER DANO INDIRETO, INCIDENTAL OU CONSEQÜENTE DE QUALQUER NATUREZA INCLUINDO, SEM LIMITAÇÃO, PREJUÍZOS POR PERDAS E DANOS, INTERRUPÇÃO DO TRABALHO, FALHA OU MAU FUNCIONAMENTO DO COMPUTADOR, OU QUAISQUER OUTROS DANOS OU PERDAS. EM NENHUM CASO A NETWORK ASSOCIATES SERÁ RESPONSABILIZADA POR QUAISQUER DANOS ACIMA DO PREÇO DE VENDA QUE A NETWORK ASSOCIATES COBRA POR UMA LICENÇA DO SOFTWARE, MESMO QUE A NETWORK ASSOCIATES TENHA SIDO AVISADA SOBRE A POSSIBILIDADE DE TAIS DANOS. O LIMITE DE RESPONSABILIDADE NÃO DEVE SER APLICADO À RESPONSABILIDADE POR MORTE OU FERIMENTOS PESSOAIS DENTRO DOS LIMITES LEGAIS EM VIGOR QUE PROÍBEM TAIS LIMITAÇÕES. ALÉM DISSO, ALGUNS ESTADOS E JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO OU LIMITAÇÃO DE DANOS INCIDENTAIS OU CONSEQÜENTES, POR ISSO TAL

LIMITAÇÃO E EXCLUSÃO PODE NÃO SE APLICAR A VOCÊ. As cláusulas anteriores serão aplicadas dentro dos limites máximos permitidos pela legislação em vigor.

8. **Governo dos Estados Unidos.** O Software e a Documentação que o acompanha são considerados “software comercial de computador” e “documentação comercial de software de computador”, respectivamente, de acordo com a Seção 227.7202 do DFAR e a Seção 12.212 do FAR conforme aplicável. Qualquer uso, modificação, reprodução, versão, execução, exibição ou divulgação do Software e da Documentação, que o acompanha, pelo Governo dos Estados Unidos serão governadas somente pelos termos deste Contrato e proibidas exceto no âmbito expressamente permitido pelos termos deste Contrato.

9. **Controles de Exportação.** É proibido exportar, reexportar ou fazer download do Software, da Documentação, das informações ou tecnologia neles contidas de nenhum modo (i) para (ou para um cidadão ou residente de) Cuba, Irã, Iraque, Líbia, Coréia do Norte, Sudão, Síria ou qualquer país para o qual os Estados Unidos da América tenham estabelecido embargo de produtos; ou (ii) para qualquer pessoa que conste na lista de Nações Especialmente Designadas (Specially Designated Nations) do Departamento do Tesouro Americano ou na Tabela de Pedidos Negados (Table of Denial Orders) do Departamento de Comércio Americano. Ao fazer download ou usar o Software, você estará aceitando as cláusulas anteriores e certificando que não está localizado em, sob o controle de, ou é cidadão ou residente em nenhum desses países, ou não consta das listas supra citadas.

   ALÉM DISSO, VOCÊ DEVE ESTAR CIENTE DE QUE A EXPORTAÇÃO DO SOFTWARE PODE ESTAR SUJEITA A COMPATIBILIDADE COM AS REGRAS E NORMAS PROMULGADAS PERIODICAMENTE PELO BUREAU OF EXPORT ADMINISTRATION DO DEPARTAMENTO DE COMÉRCIO DOS ESTADOS UNIDOS DA AMÉRICA, QUE RESTRINGE A EXPORTAÇÃO E REEXPORTAÇÃO DE DETERMINADOS PRODUTOS E DADOS TÉCNICOS. SE A EXPORTAÇÃO DO SOFTWARE FOR CONTROLADA POR ESTAS REGRAS E NORMAS, ENTÃO O SOFTWARE NÃO DEVE SER EXPORTADO OU REEXPORTADO, DIRETA OU INDIRETAMENTE, (A) SEM TODAS AS LICENÇAS PARA EXPORTAÇÃO OU REEXPORTAÇÃO E AS APROVAÇÕES GOVERNAMENTAIS DOS ESTADOS UNIDOS DA AMÉRICA OU OUTRAS PERTINENTES DITADAS POR QUAISQUER LEIS APLICÁVEIS, OU (B) VIOLANDO QUALQUER PROIBIÇÃO APLICÁVEL À EXPORTAÇÃO OU REEXPORTAÇÃO DE QUALQUER PARTE DO SOFTWARE. ALGUNS PAÍSES FAZEM RESTRIÇÕES AO USO DE CRIPTOGRAFIA DENTRO DE SUAS FRONTEIRAS, OU À IMPORTAÇÃO OU EXPORTAÇÃO DE CRIPTOGRAFIA MESMO QUE SOMENTE PARA USO COMERCIAL OU PESSOAL TEMPORÁRIO. VOCÊ ESTÁ DE ACORDO QUE A IMPLEMENTAÇÃO E O CUMPRIMENTO DESSAS LEIS NEM SEMPRE É CONSISTENTE EM RELAÇÃO A PAÍSES ESPECÍFICOS. EMBORA OS SEGUINTES PAÍSES NÃO CONSTITUAM UMA LISTA EXAUSTIVA, PODEM EXISTIR RESTRIÇÕES À EXPORTAÇÃO DE TECNOLOGIA CRIPTOGRAFADA PARA, OU IMPORTAÇÃO DA: BÉLGICA, CHINA (INCLUINDO HONG KONG), FRANÇA, ÍNDIA, INDONÉSIA, ISRAEL, RÚSSIA, ARÁBIA SAUDITA, CINGAPURA E CORÉIA DO SUL. VOCÊ CONFIRMA QUE É DE SUA RESPONSABILIDADE CUMPRIR AS LEIS DE EXPORTAÇÃO DO GOVERNO E

OUTRAS LEIS APLICÁVEIS, E QUE A NETWORK ASSOCIATES NÃO TEM MAIS NENHUMA RESPONSABILIDADE APÓS A VENDA INICIAL PARA VOCÊ NO TERRITÓRIO DE ORIGEM DA VENDA.

10. **Atividades de Alto Risco.** O Software não é tolerante a falhas e não foi projetado nem se destina ao uso em ambientes perigosos que necessitem de dispositivos de proteção contra falhas, incluindo mas não se limitando, a operação de plantas nucleares, navegação aérea ou sistemas de comunicação, controle de tráfego aéreo, sistemas de armamentos, máquinas de suporte direto à vida, ou qualquer outra aplicação na qual uma falha do software possa causar a morte, danos pessoais ou severos danos físicos ou de propriedade (coletivamente chamadas de "Atividades de Alto Risco"). A Network Associates renuncia expressamente a qualquer garantia, expressa ou implícita de adequação a Atividades de Alto Risco.

11. **Diversos.** Este Contrato é regido pelas leis dos Estados Unidos e do Estado da Califórnia, sem fazer referência a conflitos dos princípios legais. A aplicação da United Nations Convention of Contracts for the International Sale of Goods está expressamente excluída. O Contrato estabelecido neste documento tem caráter de recomendação e não substitui as cláusulas de qualquer Contrato estabelecido nos arquivos README.1ST e LICENSE.TXT, ou qualquer outro arquivo de texto que acompanhe o Software e pretenda estabelecer os termos do seu contrato de licença. Nos casos em que as cláusulas deste Contrato entrem em conflito com as cláusulas do documento README.1ST ou LICENSE.TXT, o documento de texto se constituirá nos termos da sua concessão de licença para uso do Software. Este Contrato não pode ser modificado, exceto através de um adendo por escrito, emitido por um representante da Network Associates devidamente autorizado. Nenhuma cláusula a este respeito pode ser desconsiderada a menos que essa desistência de direito seja feita por escrito e assinada pela Network Associates ou pelo seu representante devidamente credenciado. Se qualquer cláusula deste Contrato for invalidada, o restante deste Contrato continuará em vigor. As partes confirmam que é de seu desejo que este Contrato seja redigido somente em Português.

12. **Contato para o Cliente da Network Associates.** Se você tiver perguntas a fazer sobre esses termos e condições, ou se quiser entrar em contato com a Network Associates por outra razão, ligue para (408) 988-3832, fax (408) 970-9727, escreva para a Network Associates, Inc. no endereço 3965 Freedom Circle, Santa Clara, California 95054, EUA, ou visite o site da Web da Network Associates em http://www.nai.com.

Tabela de Conteúdo

Prefácio

O que aconteceu?

Se você já perdeu arquivos importantes armazenados no seu disco rígido, vendo-os desaparecer enquanto o seu computador pára a fim de exibir uma saudação juvenil de uma pessoa maliciosa no seu monitor, ou se passou pela situação de ter que se desculpar por causa de mensagens de correio eletrônico insultantes nunca enviadas, saberá em primeira mão como os vírus de computador e outros programas destrutivos podem interromper a sua produtividade. Se o seu computador ainda não tiver sido infectado por vírus, você pode colocar-se entre os que têm sorte. Porém, com mais de 24.000 vírus conhecidos em circulação, capazes de atacar sistemas de computador com base em Windows e DOS, trata-se apenas de uma questão de tempo para que isto aconteça com você.

A boa notícia é que, dos milhares de vírus circulantes, apenas um pequeno número tem meios para causar danos reais aos seus dados. De fato, o termo “vírus de computador” identifica uma ampla lista de programas que têm somente um recurso em comum: “reproduzirem-se” automaticamente ao anexarem-se ao software host ou aos setores de disco de seu computador, normalmente, sem o seu conhecimento. A maioria dos vírus causa problemas relativamente triviais, que variam dos que apenas perturbam aos completamente insignificantes. Freqüentemente, a principal conseqüência de uma infecção por vírus é o tempo e o esforço gastos para descobrir a origem da infecção e erradicar todos os seus traços.

Por que se preocupar?

Por que a preocupação com as infecções por vírus, se a maioria dos ataques causam poucos danos? O problema tem duas partes: primeira, embora relativamente poucos vírus tenham efeito danoso, isso não explica a extensão da infecção pelos vírus destrutivos. Em muitos casos, os vírus com os efeitos altamente prejudiciais são os mais difíceis de serem detectados — o programador de vírus que se dedica a causar danos tomará medidas extras para evitar a detecção. Segunda, mesmo os vírus relativamente “benignos” podem interferir na operação normal de seu computador e causar comportamentos imprevisíveis em outros softwares. Alguns vírus contêm bugs, código escrito precariamente, ou outros problemas bastante sérios que causam pane quando são executados. Outras vezes, softwares legítimos têm

problema de execução quando um vírus tiver, intencionalmente ou não, alterado os parâmetros do sistema ou outros aspectos do ambiente de computação. Buscar a origem das panes ou congelamentos de sistema resultantes gasta tempo e dinheiro que poderiam ser empregados em atividades mais produtivas.

Acima desses problemas está o da percepção: uma vez infectado, o seu computador pode servir como uma origem de infecção para outros computadores. Se você trocar dados com seus colegas ou clientes freqüentemente, poderá passar à frente um vírus, sem saber, que poderia causar mais danos à sua reputação ou aos seus contatos com outras pessoas do que ao seu computador.

A ameaça dos vírus e outros softwares destrutivos é real e piora cada vez mais. Há estimativas de gastos de US 1 bilhão por ano, no mundo inteiro, com perda de tempo e produtividade simplesmente para detectar e limpar infecções por vírus, e esta cifra não engloba os custos com a perda e recuperação de dados durante os ataques que os destruíram.

Qual a origem dos vírus?

Quando você ou um de seus colegas recupera o sistema de um ataque de vírus ou ouve falar de novas formas de softwares destrutivos que aparecem em programas usados comumente, deve se perguntar como nós, usuários de computadores, chegamos a esse ponto. Qual a origem dos vírus e de programas destrutivos? Quem os escreve? Por que aqueles que os criam procuram interromper o fluxo de trabalho, destruir dados ou fazer com que pessoas percam tempo e dinheiro para erradicá-los? O que pode fazê-los parar?

Por que isso aconteceu comigo?

Não deve ser um grande consolo ouvir que o programador que criou o vírus que apagou a tabela de alocação de arquivos do seu disco rígido não visava você ou o seu computador especificamente. Nem será motivo de alento saber que o problema com o vírus será provavelmente sempre nosso. Mas conhecer um pouco do histórico dos vírus de computador e como atuam pode ajudar a proteger melhor o seu sistema contra esses ataques.

Antecedentes dos vírus

Os pesquisadores de vírus identificaram alguns programas que incorporavam recursos agora associados a vírus de software. O educador e pesquisador canadense, Robert M. Slade, traça a linhagem dos vírus desde os utilitários com objetivos específicos usados para recuperar espaço em disco, ocupados por arquivos que não eram utilizados, e executar outras tarefas úteis nos

computadores ligados em rede mais antigos. Slade relata que os cientistas de computadores em um departamento de pesquisa da Xerox Corporation chamavam programas como esses de “vermes”, um termo usado depois que os cientistas notaram “orifícios” em mapas de memória de computador impressos, que eram semelhantes aos produzidos por vermes que os tivessem perfurado. O termo ainda é utilizado para descrever programas que se reproduzem, mas não alteram software host.

Uma forte tradição acadêmica de pregar peças através de computadores é a explicação mais provável do desvio da atenção dos programas utilitários em direção a usos mais destrutivos das técnicas de programação encontradas nos softwares “vermes”. Os estudantes de informática, para testar as suas habilidades programáticas, constróem programas “vermes” travessos e desencadeiam-nos para “lutar” entre si, competindo para ver qual programa “sobreviveria” aos rivais. Esses mesmos estudantes também encontraram utilidades para programas “vermes” nas peças pregadas em colegas confiantes.

Alguns desses estudantes logo descobriram que poderiam usar certos recursos do sistema operacional do computador host para conceder-lhes acesso não autorizado aos recursos do computador. Outros se aproveitaram de usuários que tinham relativamente pouco conhecimento de computadores para substituir seus programas — escritos com objetivos específicos — por utilitários inócuos ou comuns. Esses usuários simples executariam esses utilitários como se fossem os softwares usados rotineiramente e descobririam que seus arquivos foram apagados, suas senhas de contas roubadas ou sofreriam outras conseqüências desagradáveis. Esses programas do tipo “cavalo de Tróia” ou “troianos”, assim chamados por sua semelhança metafórica com o presente que os antigos gregos ofereceram à cidade de Tróia, continuam a ser uma ameaça significativa para os usuários de computadores atuais.

Vírus e a revolução dos PCs

O que agora conhecemos como um verdadeiro vírus de computador apareceu, inicialmente, segundo Robert Slade, logo depois que os primeiros computadores pessoais alcançaram o mercado de massa no início dos anos 80. Outros pesquisadores datam o advento dos programas de vírus em 1986, quando apareceu o vírus “Brain”. Não importa a data inicial, o vínculo entre a ameaça dos vírus e o computador pessoal não é acidental.

A nova distribuição em massa dos computadores significou que os vírus poderiam se espalhar em muito mais hosts que anteriormente, quando um número comparativamente pequeno de sistemas de grande porte altamente protegidos dominava o espaço da computação a partir de suas fortalezas em grandes corporações e universidades. Não havia necessidade dos usuários

individuais de computador, que compravam PCs, adotarem medidas de segurança sofisticadas utilizadas para proteger dados sensíveis nesses ambientes. Como um catalisador adicional, os criadores de vírus acharam relativamente mais fácil explorar algumas tecnologias de PC para serem usadas em seus próprios objetivos.

Vírus de setor de inicialização

Os PCs antigos, por exemplo, eram inicializados ou carregavam os seus sistemas operacionais a partir de disquetes. Os autores do vírus Brain descobriram que poderiam substituir os seus programas pelo código executável presente no setor de inicialização de cada disquete formatado com o MS-DOS da Microsoft, incluindo ou não os arquivos de sistema. Com isso, os usuários carregavam o vírus na memória sempre que iniciavam seus computadores com qualquer disquete formatado em suas unidades de disco. Uma vez colocado na memória, um vírus poderia se reproduzir em setores de inicialização de outros disquetes ou discos rígidos. Aqueles que inadvertidamente carregaram o vírus Brain a partir de um disquete infectado se encontraram lendo uma “propaganda” substituto para uma companhia de consultoria de informática no Paquistão.

Com essa propaganda, o Brain foi pioneiro de outro recurso característico dos vírus modernos: a carga explosiva. Essa carga é a “piada” ou comportamento destrutivo que, se for ativado, causa efeitos que variam de mensagens desagradáveis a destruição de dados. É a característica do vírus que chama mais atenção — muitos autores de vírus agora escrevem-nos especificamente para colocar sua carga explosiva no maior número possível de computadores.

Durante algum tempo, os descendentes sofisticados desse primeiro vírus de setor de inicialização representaram a maior ameaça para os usuários de computador. Variações de vírus de setor de inicialização também infectam o Registro de inicialização principal (MBR), que armazena as informações sobre partição, das quais o computador necessita para saber onde encontrar cada uma das partições do seu disco rígido e o setor de inicialização.

Na verdade, quase todos os procedimentos de inicialização, da leitura do MBR ao carregamento do sistema operacional, são vulneráveis a sabotagem por vírus. Alguns dos mais tenazes e destrutivos vírus ainda incluem a habilidade para infectar o setor de inicialização do seu computador ou do MBR no seu repertório de truques. Entre outras vantagens, a carga durante a inicialização pode dar a oportunidade ao vírus de fazer o seu trabalho antes que o seu software antivírus possa ser executado. O VirusScan antecipa essa possibilidade permitindo que você crie um disco de emergência, que pode ser usado para inicializar o computador e remover infecções.

Mas os vírus do setor de inicialização e do MBR têm uma fraqueza particular: podem se espalhar através de disquetes ou de outra mídia removível, mantendo-se ocultos na primeira trilha do espaço do disco. Como poucos usuários trocam disquetes e como a distribuição de softwares agora baseia-se em outras mídias, como CD-ROMs, outros tipos de vírus eclipsaram recentemente a ameaça ao setor de inicialização. A popularidade dos discos de alta capacidade, como o Iomega Zip e outros discos semelhantes de outros fornecedores, podem, contudo causar um ressurgimento.

Vírus infectantes de arquivos

Mais ou menos ao mesmo tempo em que os autores do vírus Brain encontraram vulnerabilidades no setor de inicialização do DOS, outros criadores de vírus descobriram como usar o software existente para ajudá-los a replicar os seus vírus. Um exemplo antigo desse tipo de vírus apareceu em computadores na Universidade de Lehigh na Pensilvânia. O vírus infectava parte do interpretador de comando DOS, COMMAND.COM, que costumava ser usado para se carregar na memória. Uma vez carregado, propagava-se por outros arquivos COMMAND.COM não infectados sempre que um usuário digitasse algum comando DOS padrão que envolvesse acesso ao disco. Isso limitava a sua propagação aos disquetes que continham, normalmente, um sistema operacional completo.

O vírus posteriores rapidamente ultrapassaram essa limitação, à vezes com programas bem mais inteligentes. Os criadores de vírus podem, por exemplo, fazer com que os vírus adicionem o seu código no início de um arquivo executável, a fim de que, quando os usuários iniciarem um programa, o código do vírus é executado imediatamente, em seguida, transfere o controle de volta para o software legítimo, que é executado como se nada de incomum tivesse acontecido. Uma vez ativado, o vírus “fisga” ou “captura” as solicitações que o software legítimo faz ao sistema operacional e substitui as suas respostas. Especificamente, os vírus mais inteligentes podem, até mesmo, subverter as tentativas de limpá-los da memória capturando a seqüência de teclado CTRL+ALT+DEL para uma reinicialização a quente, produzindo, em seguida, um reinício falso. Às vezes, somente uma indicação externa que algo no sistema estava errado — antes que qualquer carga explosiva detonasse — isto é, uma pequena modificação no tamanho de arquivo do software legítimo infectado.

Vírus de “atuação furtiva”, mutantes, criptografados e polimorfos

Discretos como devem ser, as alterações no tamanho de arquivo e outras evidências esparsas de uma infecção por vírus geralmente fornecem à maioria dos softwares antivírus pistas suficientes para localizar e remover o código ofensivo. Contudo, um dos maiores desafios para o criador de vírus é encontrar os modos de ocultar o seu trabalho. Os disfarces mais antigos se constituíam em uma mistura de programação inovadora e revelações óbvias.

O vírus Brain, por exemplo, redirecionava as solicitações de visualização de um setor de inicialização do disco para fora da localização real do setor infectado, enviando-a para a nova localização dos arquivos de inicialização deslocada pelo vírus. Essa capacidade de "atuação furtiva" habilitava este e outros vírus a ocultar-se das técnicas de busca tradicionais.

Como os vírus precisavam evitar a reinfecção contínua dos sistemas do host — isso iria aumentar rapidamente o tamanho de um arquivo infectado em proporções facilmente detectáveis ou consumiriam recursos de sistema suficientes que apontariam uma origem óbvia — seus autores também necessitavam instruí-los para deixar certos arquivos intocados. Eles abordaram esse problema fazendo com que o vírus escrevesse uma "assinatura" de código que marcaria os arquivos infectados com o sinal de software equivalente a "não perturbe". Embora esse procedimento evitasse que o vírus fosse revelado imediatamente, abriu caminho para que os softwares antivírus usassem também assinaturas de código para encontrar os vírus.

Em resposta, os criadores de vírus encontraram maneiras de esconder as assinaturas de código. Alguns vírus "mudariam" ou escreveriam assinaturas de código diferentes a cada nova infecção. Outros criptografaram a maioria das assinaturas de código ou o vírus em si, deixando apenas alguns bytes para serem usados como uma chave para a descodificação. Os novos vírus mais sofisticados empregaram a atuação furtiva, mutação e criptografia para aparecer em quase todas as variedades não detectáveis de novas formas. A localização desses vírus "polimorfos" precisavam da atuação de engenheiros de software para desenvolverem técnicas de programação muito elaboradas a fim de criar softwares antivírus.

Vírus de macro

Em torno de 1995, a guerra contra os vírus chegou a uma pausa. Novos vírus apareceram continuamente, ajudados em parte pela disponibilidade dos kits de vírus já prontos que habilitaram algumas pessoas que não eram programadores a criar um novo vírus instantaneamente. A maioria dos softwares antivírus existentes, contudo, podia ser facilmente atualizada para detectar e remover as variações do novo vírus, que consistiam basicamente de pequenos ajustes finos em modelos bem conhecidos.

Mas 1995 presenciou também o aparecimento do vírus Concept, que representou uma nova e surpreendente virada na história dos vírus. Antes do Concept, a maioria dos pesquisadores de vírus pensavam que os arquivos de dados — o texto, a planilha eletrônica ou documentos de desenho criados pelo software utilizado — eram imunes às infecções. Acima de tudo, os vírus são programas e, como tal precisavam ser executados da mesma forma que os softwares executáveis para poder causar danos. Por outro lado, os arquivos de dados, armazenavam simplesmente as informações digitadas quando o software era utilizado.

Essa distinção desapareceu quando a Microsoft começou a adicionar recursos de macro no Word e Excel, os seus principais aplicativos do conjunto Office. Usando essa versão despojada da sua linguagem Visual BASIC incluída no conjunto, os usuários podiam criar modelos de documentos que formatariam e incluiriam outros recursos aos documentos criados com o Word e Excel. Os criadores de vírus aproveitaram a oportunidade que isto apresentava para ocultar e espalhar os vírus em documentos que você, o usuário, criou.

A explosão da popularidade dos softwares de Internet e de correio eletrônico, que permitiu aos usuários anexar arquivos a mensagens, assegurou que os vírus de macro seriam difundidos muito rápido e amplamente. Em um ano, os vírus de macro tornaram-se as ameaças mais potentes jamais vistas.

Dentro do limite

Enquanto os vírus tornam-se mais sofisticados e continuam a ameaçar a integridade dos sistemas de computador dos quais acabamos tendo que depender, já outros perigos começam a emergir de uma fonte inesperada: a World Wide Web. Originalmente um repositório de pesquisas e tratados acadêmicos, a Web transformou-se no meio mais adaptável e versátil já inventado para comunicação e comércio.

Como o seu potencial parece bem amplo, a Web chamou a atenção e canalizou os esforços de desenvolvimento de quase todas as empresas relacionadas a computadores da indústria. As tecnologias convergentes que resultaram desse ritmo febril de invenções agora forneceram as ferramentas aos designers de páginas da Web, que podem ser usadas para coletar e exibir informações de modos nunca antes disponíveis. Atualmente, os sites da Web podem enviar e receber correio eletrônico, formular e realizar pesquisas em bancos de dados usando mecanismos de busca avançados, enviar e receber áudio e vídeo ativo, e distribuir dados e recursos de multimídia para um público mundial.

Muita dessa tecnologia que possibilita a existência desses recursos consiste de pequenos programas que podem ser obtidos por download e que interagem com o seu software de navegação e, à vezes, com outro software no disco rígido. Este mesmo caminho pode servir como um ponto de entrada de outros programas no sistema do computador— menos benignos — que os usam com objetivos próprios.

Java e ActiveX

Esses programas, benéficos ou destrutivos, apresentam-se de várias formas. Alguns são miniaplicativos para um objetivo específico, ou “applets”, escritos em Java, uma nova linguagem de programação, desenvolvida inicialmente pela Sun Microsystems. Outros são desenvolvidos usando a ActiveX, uma tecnologia da Microsoft que os programadores podem usar com propósitos semelhantes.

As classes Java e os controles ActiveX fazem amplo uso de módulos de software pré-escritos, ou “objetos”, que os programadores podem escrever ou obter de origens existentes e adaptá-los aos plug-ins, miniaplicativos, controladores de dispositivos e outros softwares necessários a capacitar a web. Os objetos Java são chamados “classes”, enquanto os objetos ActiveX são chamados “controles”. A principal diferença entre eles é a forma como são executados no sistema do host. Os miniaplicativos Java são executados em uma “máquina virtual” Java projetada especialmente para interpretar essa programação e convertê-la em ações na máquina host, enquanto que os controles ActiveX são executados como programas nativos do Windows e passam dados entre outros programas do Windows.

A grande maioria desses objetos é parte útil e, até mesmo, necessária, de qualquer site da Web interativo. Mas apesar dos melhores esforços dos engenheiros da Sun e da Microsoft para embutir medidas de segurança nessas tecnologias, programadores mal-intencionados podem usar as ferramentas Java e a ActiveX para introduzir objetos destrutivos nos sites da Web, onde podem esconder-se até que visitantes involuntariamente lhes permitam acessar sistemas de computadores vulneráveis.

A contrário dos vírus, os objetos nocivos Java e ActiveX não têm, em geral, como principal objetivo a auto-replicação. A Web lhes dá muitas oportunidades para se espalharem em sistemas de computadores de destino, enquanto que seu tamanho pequeno e natureza inócua lhes facilita driblar a detecção. De fato, a menos que você instrua especificamente o seu navegador web para bloqueá-los, os objetos Java e ActiveX serão descarregados automaticamente no sistema sempre que um site da web que os hospeda for visitado.

Ao invés disso, os objetos destrutivos existem para passar o seu equivalente de carga explosiva. Os programadores escreveram objetos que podem, por exemplo, ler dados em seu disco rígido e enviá-los de volta para o site da web que você visitou, “seqüestrar” a sua conta de correio eletrônico e enviar mensagens ofensivas em seu nome, ou observar os dados que passam do seu computador para outros computadores.

Qual é a próxima etapa?

Os softwares destrutivos começaram a introduzir-se até mesmo em áreas que se pensava estarem completamente fora dos limites de infecção. Os usuários do cliente mIRC Internet Relay Chat, por exemplo, relataram ter encontrado vírus construídos a partir da linguagem de script mIRC. O cliente do Chat envia vírus de script como texto simples, o que normalmente impede que infectem sistemas, porém as versões mais antigas do software de cliente mIRC interpretavam as instruções codificadas no script e executavam ações indesejadas no computador do destinatário. Os fornecedores decidiram rapidamente desativar esse recurso nas versões atualizadas do software, mas o incidente com o mIRC ilustra a regra geral que estabelece que onde há um modo de explorar uma brecha na segurança de um software, alguém a encontrará e usará.

Alguns criadores de vírus fazem-no somente pela emoção que isso possa produzir ou para ganhar notoriedade em seu grupo. Outros, ainda, para se vingar de funcionários ou de pessoas que eles pensam os terem maltratado. Não importam os motivos, eles continuam a desenvolver novas maneiras de lhe causar problemas.

Como proteger o sistema

A proteção avançada do VirusScan já fornece uma importante proteção contra infecções e danos aos seus dados, mas o software antivírus é apenas uma parte das medidas de segurança que você deve tomar para proteger os seus dados. Além disso, um software antivírus é bom apenas enquanto vigora a sua última atualização. Como aparecem de 200 a 300 vírus e suas variantes por mês, os arquivos (.DAT) de dados que habilitam o software da Network Associates a detectar vírus e remover vírus poderão ficar rapidamente desatualizados. Se você não atualizar os arquivos contidos no produto original, poderá arriscar-se a infecções em seu sistema por novos vírus emergentes. Como a Network Associates formou a maior e mais experiente equipe de pesquisa antivírus do mundo na divisão McAfee Labs, os arquivos atualizados e necessários para combater novos vírus aparecem assim - ou mesmo antes - que você necessite deles.

A maioria das medidas de segurança são de senso comum — o exame de discos recebidos de origem desconhecida ou questionável, usando um software antivírus ou algum tipo de utilitário de verificação, é sempre uma boa idéia. Os programadores destrutivos chegaram até a imitação de programas, que você acredita estarem protegendo o seu computador, apresentando-os com uma aparência familiar, porém com objetivos que estão longe de serem amistosos. O VirusScan inclui o utilitário VALIDATE.EXE com suas distribuições para impedir esse tipo de manipulação, mas nem ele nem o software antivírus podem detectar quando alguém substitui um de seus de seus utilitários comerciais ou shareware favoritos por um programa destrutivo ou do tipo cavalo de Tróia que ainda não tenha sido identificado.

O acesso à Internet e à Web apresenta os seus próprios riscos. O VirusScan possibilita o bloqueio de sites da web perigosos para que os usuários não possam, inadvertidamente, fazer download de um software destrutivo em sites prejudiciais conhecidos; esse programa também captura objetos hostis que são descarregados de qualquer modo. É uma necessidade colocar uma barreira de proteção de primeira linha para a sua rede e implementar outras medidas de segurança quando atacantes inescrupulosos podem penetrar em sua rede a partir de quase todos os pontos do globo, para roubar dados sensíveis ou implantar códigos destrutivos. Você também deve assegurar que a sua rede não esteja acessível a usuários não autorizados e que tenha sido implementado um programa em seu local de trabalho para ensinar e reforçar os padrões de segurança. Para saber mais sobre a origem, o comportamento e outras características dos vírus, consulte a Biblioteca de informações sobre vírus mantida no site da Web da Network Associates.

A Network Associates pode fornecer-lhe outros softwares do conjunto Total Virus Defense (TVD), a mais completa solução antivírus disponível, e Total Network Security (TNS), o conjunto de segurança de rede mais avançado da indústria. A Network Associates os apóia com suporte amplo, treinamento e uma rede mundial de equipes de pesquisa e desenvolvimento. Entre em contato com o seu representante da Network Associates ou visite o site da Web da empresa, para saber como usar os recursos avançados da Total Virus Defense em seu sistema.

Como entrar em contato com a Network Associates

Atendimento ao cliente

Para encomendar produtos ou obter informações sobre produtos, entre em contato com o Departamento de Atendimento ao Cliente da Network Associates no telefone (011) 550-51009 ou escreva para os seguintes endereços:

Network Associates, Inc.
McCandless Towers
Rua Geraldo Flauzino Gomes 78-cj.
São Paulo, SP 04575-060
Brasil

Suporte técnico

A Network Associates é famosa pela dedicação à satisfação do cliente. Mantemos essa tradição tornando o nosso site da World Wide Web um recurso valioso para a obtenção de informações sobre assuntos relativos a suporte técnico. Encorajamos os nossos clientes a fazer desta a sua primeira parada para obter respostas a perguntas freqüentes, atualizações do software da Network Associates e acesso a novidades e informações sobre vírus.

World Wide Web	http://www.nai.com

Se você não encontrar o que precisa ou não tiver acesso à Web, experimente um de nossos serviços automatizados.

Sistema de resposta de fax e voz automatizado	(408) 988-3034
Internet	support@nai.com
CompuServe	GO NAI
America Online	palavra-chave MCAFEE

Se os serviços automatizados não contiverem as respostas necessárias, entre em contato com a Network Associates através de um dos seguintes telefones, de segunda a sexta, das 6:00 às 18:00, Hora do Pacífico.

Para clientes com licença corporativa:

Telefone	(408) 988-3832
Fax	(408) 970-9727

Para clientes com licença para revenda:

Telefone	(972) 278-6100
Fax	(408) 970-9727

Para fornecer as respostas que você precisa de maneira rápida e eficiente, a equipe de suporte técnico da Network Associates precisa de algumas informações sobre o seu computador e o software. Tenha estas informações à mão antes de ligar:

- n
- Marca e modelo do computador
- -{}--{}-n
- Números do tipo e da versão do sistema operacional
- Tipo e versão da rede, se for aplicável
- Conteúdo do AUTOEXEC.BAT, CONFIG.SYS e script de LOGIN do seu sistema
- Etapas específicas para reproduzir o problema

Treinamento da Network Associates

Para obter informações sobre planejamento de treinamento no local para qualquer produto da Network Associates, ligue para 00 1 (800) 338-8754.

Comentários e sugestões

A Network Associates aprecia os seus comentários e reserva-se o direito de usar qualquer informação que você fornecer da maneira mais adequada sem incorrer em qualquer obrigação para com o cliente. Envie seus comentários sobre a documentação do produto antivírus da Network Associates para: Network Associates, Inc., 15220 NW Greenbrier Parkway, Suite 100, Beaverton, OR 97006-5762, EUA. Você também pode enviar seus comentários via fax para o telefone (503) 531-7655 ou correio eletrônico para tvd_documentation@nai.com.

Relatando novos itens para atualizações de arquivos de dados de antivírus

O software antivírus da Network Associates oferece os melhores recursos de detecção e remoção de vírus disponíveis, incluindo a varredura heurística avançada que pode detectar novos vírus ainda não nomeados à medida que surgirem. Contudo, ocasionalmente, um tipo inteiramente novo de vírus, que não é uma variação de um outro mais antigo, pode aparecer no seu sistema e escapar à detecção. Como os pesquisadores da Network Associates estão empenhados em lhe fornecer ferramentas eficientes e atualizadas que possam ser usadas para proteger o seu sistema, informe-os sobre quaisquer novas classes Java, controles ActiveX, sites da web perigosos ou vírus que o seu software ainda não detecta. Observe que a Network Associates se reserva o direito de usar as informações fornecidas pelos clientes da forma que achar mais adequada, sem incorrer em nenhuma obrigação com relação ao usuário. Envie suas sugestões para:

virus_research@nai.com	Use esse endereço para relatar novos tipos de vírus, controles ActiveX e classes Java prejudiciais, ou sites da Internet perigosos.

Para relatar itens ao nosso escritório de pesquisa europeu, use este endereço de correio eletrônico:

virus_research_europe@nai.com

Para fazer relatos ao nosso escritório de pesquisa na Ásia do Pacífico ou ao nosso escritório no Japão, use um destes endereços de correio eletrônico:

avert-jp@nai.com	Use este endereço para fazer o relato sobre itens destrutivos ao nosso escritório no Japão.
avert_apac@nai.com	Use este endereço para relatar itens destrutivos ao nosso escritório na Ásia do Pacífico.

Informações sobre contato internacional

Para entrar em contato com a Network Associates fora dos Estados Unidos, use os endereços e números de telefone e fax abaixo.

Net Tools Network Associates
África do Sul

Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
África do Sul 2021
Tél.: 27 11 706-1629
Fax: 27 11 706-1569

Network Associates
Austrália

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Austrália 2065
Tél.: 61-2-8425-4200
Fax: 61-2-9439-5166

Network Associates
Áustria

Pulvermuehlstrasse 17
Linz, Áustria
Postal Code A-4040
Tél.: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates
Bélgica

Bessenveldtstraat 25a
Diegem
Bélgica - 1831
Tél.: 32-2-716-4070
Fax: 32-2-716-4770

Network Associates
Brasil

Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasil
Tél.: (55 11) 5505 1009
Fax: (55 11) 5505 1006

Network Associates
Canadá

139 Main Street, Suite 201
Unionville, Ontario
Canadá L3R 2G6
Tél.: (905) 479-4189
Fax: (905) 479-4540

Network Associates Deutschland GmbH

Industriestrasse 1
D-82110 Germering
Alemanha
Tél.: 49 8989 43 5600
Fax: 49 8989 43 5699

Network Associates Espanha

Orense 4, quarto assoalho
Edificio Trieste
28020 Madrid
Espanha
Tél.: 34 91 598 18 00
Fax: 34 91 556 14 01

NA Network Associates Oy Finlândia

Kielotie 14 B
01300 Vantaa
Finlândia
Tél.: 358 9 836 2620
Fax: 358 9 836 26222

Network Associates France S.A.

50 rue de Londres
75008 Paris
França
Tél.: 33 1 44 908 737
Fax: 33 1 45 227 554

Network Associates Hong Kong

19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Tél.: 852-2832-9525
Fax: 852-2832-9530

Network Associates International B.V.

Gatwickstraat 25
1043 GL Amsterdam
Paises Baixos
Tél.: 31 20 586 6100
Fax: 31 20 586 6101

Network Associates International Ltd.

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EG
Reino Unido
Tél.: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

Network Associates Srl Italie

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italie
Tél.: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

Network Associates
Japan, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001 Japão
Tél.: 81 3 5408 0700
Fax: 81 3 5408 0781

Network Associates
Latin America

150 South Pine Island Road, Suite 205
Plantation, Florida 33324
EUA
Tél.: (954) 452-1731
Fax: (954) 236-8031

Network Associates
Mexico

Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico City, Mexico D.F. 11560
Tél.: (525) 282-9180
Fax: (525) 282-9183

Network Associates
Portugal

Av. de Liberdade, 114
1250 Lisboa
Portugal
Tél.: 351 1 340 45 43
Fax: 351 1 340 45 75

Network Associates
República Popular da China

New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Beijing
República Popular da China 100044
Tél.: 8610-6849-2650
Fax: 8610-6849-2069

Network Associates
South East Asia

7 Temasek Boulevard
The Penthouse
#44-01, Suntec Tower One
Singapore 038987
Tél.: 65-430-6670
Fax: 65-430-6671

Network Associates
Suécia

Datavägen 3A
Box 596
S-175 26 Järfälla
Suécia
Tél.: 46 (0) 8 580 88 400
Fax: 46 (0) 8 580 88 405

Network Associates AG
Suisa

Baeulerwisenstrasse 3
8152 Glattbrugg
Suisa
Tél.: 0041 1 808 99 66
Fax: 0041 1 808 99 77

Sobre o McAfee VirusScan 1

O que é o VirusScan?

O VirusScan é o elemento principal de área de trabalho do conjunto de ferramentas de segurança Total Virus Defense da Network Associates. Esse programa atua como uma sentinela online sem descanso que protege o seu sistema contra ataques de vírus e previne danos provenientes de outro software destruidor. O seu conjunto avançado de ferramentas de varredura e outros aprimoramentos o mantêm na primeira linha de softwares antivírus, porém na última versão, o VirusScan adicionou a tecnologia McAfee WebScanX ao seu arsenal protetor — uma melhoria que ajuda a manter o seu sistema a salvo das ameaças que podem começar a emergir da Internet.

Os desenhos de páginas da web avançados, por exemplo, podem incorporar elementos interativos compostos por classes Java e controles ActiveX. Ao mesmo tempo, milhões de usuários agora trocam mensagens, arquivos e outros dados via correio eletrônico, usando com freqüência "anexos" que consistem de arquivos executáveis, modelos de documentos e outros dados. Mas essas novas tecnologias convenientes também podem ocultar novos perigos. Os arquivos executáveis infectados com vírus podem ocultar-se em sites da web, muitas vezes sem o conhecimento do proprietário do site, ou podem espalhar-se via correio eletrônico, sendo ou não solicitados. Programadores sofisticados podem programar miniaplicativos Java ou controles ActiveX que burlam os recursos de segurança implementados no seu software de navegação para ler dados armazenados no disco rígido do computador, forjar mensagens de correio eletrônico para outras pessoas em seu nome ou causar outros tipos de danos.

Neste ambiente, tomar precauções para proteger o seu computador contra softwares destrutivos não é mais considerado um luxo, mas uma necessidade. Considere a extensão de sua confiança nos dados colocados em seu computador e o tempo, trabalho e dinheiro gastos para substituí-los se forem corrompidos ou inutilizados por infecção de um vírus. Compare esta possibilidade ao tempo e esforço despendidos para implementar algumas medidas de segurança comuns e você poderá ver rapidamente a utilidade de proteger o seu computador contra essas infecções.

Mesmo que os seus dados não sejam muito importantes, negligenciar a sua proteção contra vírus pode significar que o computador faça o papel de hóspede involuntário para um vírus que poderá espalhar-se pelos computadores usados pelos seus funcionários e colegas. A verificação periódica do disco rígido com o VirusScan reduz significativamente a vulnerabilidade do computador à infecção por vírus e faz com que você não perca tempo, dinheiro e dados desnecessariamente.

O VirusScan lhe fornece as ferramentas necessárias para manter o seu sistema intacto e seguro. Usado adequadamente como parte de um programa completo de segurança que inclui backups, significativa proteção por senha, treinamento e conscientização, o VirusScan pode manter o seu computador a salvo de ataques desestabilizadores e prevenir a difusão de software destrutivo em sua rede.

O que acompanha o VirusScan?

O VirusScan consiste de diversos conjuntos de componentes que combinam um ou mais programas relacionados, cada um deles desempenhando um papel na defesa do seu computador contra vírus e outros softwares destrutivos. Os conjuntos de componentes são:

- **Componentes Comuns.** Este conjunto de arquivos de dados e de outros arquivos de suporte são compartilhados por muitos componentes de programa do VirusScan. Esses arquivos incluem os arquivos (.DAT) de definição de vírus do VirusScan, arquivos de configuração padrão, arquivos de validação e outros.

- **Varredura da Linha de Comando.** Este conjunto consiste do SCANPM.EXE, um agente de varredura avançado para ambientes de 32 bits, e do BOOTSCAN.EXE, um scanner menor, especializado. Ambos os programas permitem iniciar operações de varredura específicas na janela do Prompt do MS-DOS ou no modo protegido do MS-DOS. Normalmente, você usará a interface gráfica de usuário (GUI) do VirusScan para executar a maioria das operações de varredura desse programa, mas se ocorrerem problemas na inicialização do Windows ou se os componentes GUI do VirusScan não forem executados no seu ambiente, você poderá usar as varreduras de linha de comando como um backup.

  O SCANPM.EXE fornece um scanner com recursos completos para ambientes DOS no modo protegido de 16 e 32 bits e inclui suporte para memória estendida e alocações de memória flexíveis. Para usar o scanner, abra a janela do Prompt do MS-DOS ou reinicie o seu computador no modo MS-DOS, em seguida execute o SCANPM.EXE na linha de comando, junto com as opções de varredura escolhidas. Veja Apêndice E, “Usando as opções da Linha de comando do Virus Scan,” para obter a lista e a descrição das opções disponíveis.

O VirusScan usa o BOOTSCAN.EXE no Disco de Emergência para que o seu ambiente de inicialização esteja livre de vírus. Ao executar o utilitário de criação de Disco de Emergência, o VirusScan copia o BOOTSCAN.EXE, um conjunto especializado de arquivos .DAT e os arquivos de inicialização em um único disquete. Com esse disco, você pode iniciar o computador e, em seguida, examinar a memória e o Registro de inicialização principal, o setor de inicialização e os arquivos de sistema do disco rígido.

O BOOTSCAN.EXE não detectará ou limpará os vírus de macro, porem o fará com outros vírus que podem pôr em risco a instalação do VirusScan ou os arquivos infectados na inicialização do sistema. Ao identificar e atuar sobre esses vírus, você poderá executar seguramente o VirusScan para limpar o restante do sistema, conquanto não sejam executados quaisquer outros programas durante esse procedimento.

- **VirusScan.** Este componente permite um controle inigualável sobre as operações de varredura. Você pode iniciar uma operação de varredura a qualquer momento — através de um recurso conhecido como varredura “por solicitação” — especificar os discos locais e de rede como alvos da varredura, escolher como o VirusScan atuará em relação às infecções encontradas e ver os relatórios de suas ações. O VirusScan pode ser iniciado no modo de configuração básica, em seguida mudado para o modo avançado para ter a máxima flexibilidade. Veja “Usando o McAfee VirusScan” na página 153 para obter mais detalhes.

- **VShield.** Este componente lhe oferece uma proteção antivírus contínua contra vírus originados em disquetes, inseridos através da rede ou carregados na memória. O VShield inicia quando o computador é ativado e permanece na memória até que a sessão seja fechada. Um conjunto flexível de páginas de propriedades permite informar ao VShield quais partes do sistema devem ser examinadas e quando, quais partes não devem ser examinadas e como atuar sobre os arquivos infectados que forem encontrados. Além disso, o VShield pode alertá-lo quando um vírus for encontrado e poderá gerar relatórios que resumem cada uma de suas ações.

  Esta versão mais recente do VShield inclui uma tecnologia que protege contra miniaplicativos Java e controles ActiveX hostis. Com este novo recurso, o VShield pode examinar automaticamente as mensagens de correio eletrônico e os anexos recebidos da Internet via Lotus cc:Mail, Microsoft Mail ou outros clientes de correio compatíveis com a Messaging Application Programming Interface (MAPI) da Microsoft. O programa pode também filtrar classes Java e controles ActiveX hostis comparando os que forem encontrados com um banco de dados de classes e controles conhecidos por serem nocivos. Quando são encontrados, o VShield o alerta ou pode automaticamente negar acesso ao sistema aos objetos destrutivos. O Vshield também pode impedir que o seu computador conecte-se a sites

de Internet perigosos. Basta designar os sites que o seu software de navegação não deve visitar e o VShield automaticamente impedirá o acesso. Uma proteção por senha eficiente para as opções de configurações evita que outras pessoas façam alterações não autorizadas. A mesma caixa de diálogo conveniente controla as opções de configuração para todo os módulos do VShield. Veja “Usando o VShield” na página 83 para obter detalhes.

- **Varredura do cc:Mail.** Este componente inclui a tecnologia otimizada para examinar as caixas de correio do Lotus cc:Mail que não usam o padrão MAPI. Instale e use esse componente se o seu grupo de trabalho ou a rede usar o cc:Mail v7.x ou anterior. Veja “Escolhendo opções de Detecção” na página 109 para obter mais detalhes.

- **Varredura MAPI.** Este componente permite examinar, quando você quiser, a Caixa de Entrada ou outras caixas de correio de aplicativos de clientes de correio eletrônico compatíveis com MAPI. Utilize-o para complementar a varredura em segundo plano contínua que o VShield fornece para os clientes MAPI, como Microsoft Exchange e Microsoft Outlook. Veja “Varredura de correio do Microsoft Exchange e Outlook” na página 241 para obter mais detalhes.

- **Programador de Tarefas do VirusScan.** Este componente permite criar tarefas para serem executadas pelo VirusScan. Uma “tarefa” pode incluir desde a execução de uma operação de varredura em um conjunto de discos em um momento ou intervalo específico, até a configuração do VShield para ser executado com opções específicas. O Programador de Tarefas contém uma lista predefinida de tarefas que assegura um nível mínimo de proteção para o seu sistema — você pode, por exemplo, examinar e limpar imediatamente a unidade C: ou todos os discos em seu computador, além de ativar ou desativar o VShield. Veja “Planejando tarefas de varredura” na página 183 para obter mais detalhes.

- **McAfee ScreenScan.** Este componente opcional examina o computador enquanto a proteção de tela está em execução durante os períodos de inatividade. Veja “Usando o ScreenScan” na página 258 para obter mais detalhes.

- **Documentação.** A documentação do VirusScan inclui:

  – Um *Guia de Início Rápido* impresso, que apresenta o produto, fornece informações de instalação, descreve como atuar se você suspeitar que o computador contém um vírus e dá uma visão geral resumida do produto. O *Guia de Início Rápido* é fornecido apenas com as cópias do VirusScan distribuídas nos discos de CD-ROM — você não pode obtê-lo por download no site da web da Network Associates ou em outros serviços eletrônicos.

– Esse guia do usuário pode ser salvo no CD-ROM do VirusScan ou instalado no disco rígido no formato .PDF do Adobe Acrobat. O *Guia do Usuário* do VirusScan descreve detalhadamente como usar o VirusScan e inclui outras informações úteis como segundo plano e as opções de configuração avançadas. Os arquivos .PDF do Acrobat são documentos online flexíveis que contêm hiperlinks, com descrições e outras opções de ajuda para fácil navegação e recuperação de informações.

  Para obter melhores resultados ao abrir e imprimir o *Guia do Usuário*, a Network Associates recomenda o uso do Acrobat Reader 3.0 — o Reader versão 3.0.1 tem dificuldade em imprimir corretamente os gráficos incluídos no arquivo .PDF.

– Um arquivo de ajuda online. Com esse arquivo, você pode ter acesso rápido às sugestões e dicas sobre a maneira de usar o VirusScan. Para abrir o arquivo de ajuda no VirusScan ou no Programador de Tarefas do VirusScan, escolha **Tópicos da ajuda** no menu **Ajuda**.

  O VirusScan também inclui ajuda online contextual. Clique o botão direito do mouse sobre botões, listas ou outros elementos das caixas de diálogo para ver tópicos de ajuda descritivos e resumidos. Clique nos botões **Ajuda** onde você possa vê-los para abrir o arquivo de ajuda principal em um tópico relevante.

– Um arquivo README.1ST ou LICENSE.TXT. Esse arquivo descreve os termos da sua licença para usar o VirusScan. Leia-o com atenção — ao instalar o VirusScan, você estará concordando com esses termos.

– Um arquivo WHATSNEW.TXT. Esse arquivo contém as informações mais recentes ou alterações na documentação, as listas de quaisquer comportamentos conhecidos ou outros assuntos relativos à versão do produto e, freqüentemente, descreve novos recursos do produto incorporados nas atualizações. O arquivo WHATSNEW.TXT encontra-se no nível raiz do CD-ROM do VirusScan ou na pasta de programa do VirusScan — você pode abrir e imprimi-lo no Bloco de Notas do Windows ou em quase todos os softwares de processamento de texto.

Decidindo quando examinar para descobrir vírus

Manter um ambiente de computação seguro significa examiná-lo regularmente para descobrir vírus. Dependendo da freqüência na qual você troca disquetes com outros usuários, compartilha arquivos em sua rede local ou interage com outros computadores via Internet, as varreduras "regulares" podem significar desde exames apenas mensais até diversas vezes ao dia. Outros bons hábitos a serem cultivados incluem a varredura logo antes de fazer backup dos dados, antes de instalar software novo ou cuja versão tenha sido atualizada, particularmente o software obtido por download em outros computadores e a varredura ao abrir e fechar o seu computador todos os dias. Use o VShield para examinar a memória do seu computador e manter um nível constante de vigilância entre as operações de varredura. Na maioria das circunstâncias este procedimento pode proteger a integridade do sistema.

Se você conecta-se à Internet ou faz download de arquivos freqüentemente, talvez queira implementar varreduras regulares com base em certos eventos. O VirusScan inclui um conjunto padrão de tarefas de varredura para ajudá-lo a monitorar o seu sistema nos pontos prováveis de entrada de vírus, por exemplo

- ao inserir um disquete na unidade de disco do computador
- ao iniciar um aplicativo ou abrir um arquivo
- ao conectar ou mapear uma unidade de rede ao seu sistema

Contudo, mesmo a varredura mais precisa pode deixar passar novos vírus, se o seu software de varredura não estiver atualizado. A aquisição do VirusScan lhe dá direito a atualizações de vírus grátis durante a vida de seu produto, assim você poderá atualizá-lo freqüentemente para estar em dia com os novos vírus. Se for instalado o software de cliente SecureCast da Network Associates, o VirusScan lhe informará até mesmo quando é preciso atualizar os seus arquivos de dados e se oferece para fazer o download desses arquivos para você. Para saber como atualizar o software, veja Apêndice A, "Usando o SecureCast para atualizar o software" e "Configurando as opções do AutoUpdate" na página 217.

Reconhecendo quando não há vírus

Os computadores pessoais foram desenvolvidos em sua breve existência tornando-se máquinas altamente complexas que executam softwares cada vez mais avançados. Mesmo os entusiastas de PCs mais clarividentes não poderiam imaginar as tarefas para as quais os trabalhadores, cientistas e outros conseguiram desenvolver a velocidade, flexibilidade e potência dos PCs modernos. Mas este avanço tem um preço: os conflitos entre hardware e software aumentam, os aplicativos e sistemas operacionais falham e centenas

de outros problemas podem surgir em locais improváveis. Em alguns casos, essas falhas podem assemelhar-se aos tipos de efeitos observados quando há uma infecção por vírus com conseqüências destrutivas. Outras falhas de computadores parecem desafiar explicações ou diagnósticos pelo modo frustrante com que os usuários culpam os vírus, talvez como um último recurso.

Embora os vírus deixem seus traços, você pode normalmente eliminar uma infecção por vírus como uma possível causa da falha do computador de modo relativamente rápido e fácil. Executar um sistema completo de varredura de sistema do VirusScan revelará todas as variações de vírus conhecidas que podem infectar o seu computador, e algumas que têm nome desconhecido e comportamento indefinido. Embora isso não ajude muito quando o seu problema resultar, na verdade, de um conflito de interrupções, permite eliminar uma possível causa. Com esta informação, é possível prosseguir na solução do problema do seu sistema com um utilitário de diagnóstico completo, como o McAfee Nuts & Bolts.

Mais séria é a confusão resultante dos programas semelhantes a vírus, das peças pregadas por vírus e reais quebras de segurança. O software antivírus não pode simplesmente detectar ou atuar sobre esses agentes destrutivos, como programas do tipo cavalo de Tróia que ainda não haviam aparecido, quebras de segurança que habilitam os hackers a impedir o acesso à rede e causam falhas no sistema, ou concluir que existe um vírus quando, de fato, não há nenhum.

A melhor maneira de determinar se a falha no computador é resultante de um ataque de vírus é executar uma operação de varredura completa e prestar atenção nos resultados. Se o VirusScan não relatar uma infecção por vírus, são pequenas as chances de que seja essa a causa do problema — procure outras explicações para as suas dificuldades. Além disso, no caso raro em que o VirusScan não detecta um vírus de macro ou de outro tipo que tenha infectado o seu sistema, as probabilidades são relativamente pequenas de que falhas sérias aconteçam após esse fato. Contudo, você pode confiar nos pesquisadores da Network Associates para identificar, isolar e atualizar o VirusScan imediatamente a fim de detectar e, se possível, remover o vírus ao encontrá-lo de novo. Para saber como ajudar os pesquisadores de vírus para que eles lhe ajudem, veja “Relatando novos itens para atualizações de arquivos de dados de antivírus” na página xxv.

Instalando o McAfee VirusScan 2

Antes de iniciar

A Network Associates distribui o McAfee VirusScan de duas maneiras: como um arquivo que pode ser obtido por download no site da web da Network Associates ou a partir de outros serviços eletrônicos e em forma de CD-ROM. Após fazer o download do arquivo do VirusScan ou ter colocado o disco de instalação do VirusScan na sua unidade de CD-ROM, as etapas de configuração a serem seguidas são as mesmas para cada tipo de distribuição. Reveja os requisitos de sistema mostrados abaixo para verificar se o VirusScan pode ser executado no seu sistema, em seguida realize as etapas de instalação na página 38.

NOTA: Alguns conjuntos de componentes do VirusScan são distribuídos na versão em CD-ROM do produto. Consulte o seu representante de vendas para obter mais detalhes.

Requisitos de sistema

O VirusScan poderá ser instalado e executado em qualquer PC da IBM ou em um computador compatível com PC, equipado com:

- Um processador equivalente ao Intel 80386 ou posterior. A Network Associates recomenda pelo menos um processador da classe Pentium da Intel ou compatível.
- Uma unidade de CD-ROM. Se você fizer download da sua cópia do VirusScan, esse item será opcional.
- Pelo menos 15MB de espaço livre em disco para uma instalação completa.
- Pelo menos 8MB de memória de acesso aleatório (RAM).
- Microsoft Windows 95 ou Windows 98.

Outras recomendações

Para obter todas as vantagens dos recursos de atualização automática do VirusScan, você deve ter uma conexão com a Internet através de uma rede local ou via um modem de alta velocidade e um provedor de serviços de Internet.

NOTA: A Network Associates *não* fornece conexões com a Internet. Entre em contato com o provedor de serviços local para se informar sobre preços e condições de serviço ou fale com o seu administrador de sistemas para saber como estabelecer a conexão com a Internet através da rede de seu escritório.

Etapas da instalação

Verifique qual é o seu tipo de distribuição do VirusScan, em seguida realize as etapas correspondentes para preparar os seus arquivos para instalação.

- **Se você fez download da sua cópia do VirusScan** no site da web da Network Associates, de um servidor de sua rede local ou de outro serviço eletrônico, crie uma nova pasta temporária no disco rígido, em seguida use o WinZip, PKZIP ou um assistente semelhante para extrair os arquivos de instalação do VirusScan para essa pasta temporária. Pode ser feito download dos utilitários necessários a partir da maioria dos serviços online.

  IMPORTANTE: Se você suspeitar que o seu computador foi infectado por vírus, faça download dos arquivos de instalação do VirusScan em um computador que ***não*** esteja infectado. Instale a sua cópia neste computador, em seguida use o assistente Disco de emergência da McAfee durante a configuração para criar um disco que possa ser usado para inicializar o computador infectado e remover o vírus. Veja "Se você suspeitar que há um vírus..." na página 61 para obter mais informações.

- **Se a origem de sua cópia do VirusScan for um CD-ROM**, insira esse disco na unidade correspondente.

Após inserir o CD-ROM, você deverá ver uma imagem de boas-vindas do VirusScan semelhante àquela mostrada na Figura 2-1 na página 39, que aparece automaticamente.
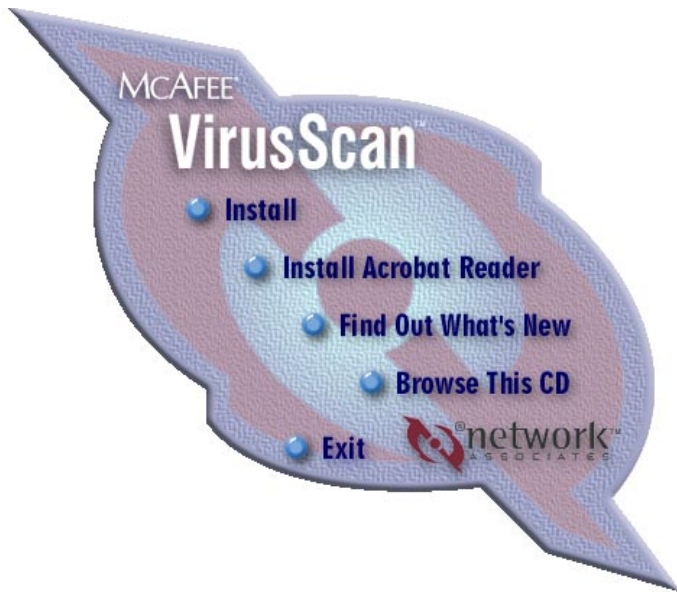
Figura 2-1. Imagem de boas-vindas da McAfee VirusScan

Para instalar o VirusScan imediatamente, clique em **Instalar** e vá para Etapa 3 na página 40 a fim de continuar a configuração.

Se a imagem de boas-vindas não aparecer ou se você estiver instalando o VirusScan a partir de arquivos obtidos por download, inicie na Etapa 1.

Siga estas etapas:

1. Escolha **Executar** no menu **Iniciar** na barra de tarefas do Windows.

   Aparecerá a caixa de diálogo Executar (Figura 2-2).
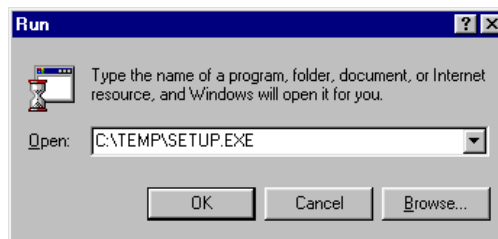
Figura 2-2. Caixa de diálogo Executar

2. Digite <X>:\SETUP.EXE na caixa de texto fornecida, em seguida clique em **OK**.

   Nessa caixa, o <X> representa a letra da sua unidade de CD-ROM ou o caminho para a pasta que contém os arquivos do VirusScan extraídos. Para procurar os arquivos corretos no seu disco rígido ou no CD-ROM, clique em **Procurar**.

   NOTA: Se a origem de sua cópia do VirusScan for um CD-ROM da VirusScan Security Suite ou Total Virus Defense, você deve especificar também qual pasta contém o VirusScan para Windows 95 e Windows 98. Veja o arquivo CONTENTS.TXT incluído neste CD-ROM para obter mais detalhes.

   O programa de configuração será iniciado e exibirá o painel de boas-vindas (Figura 2-3).
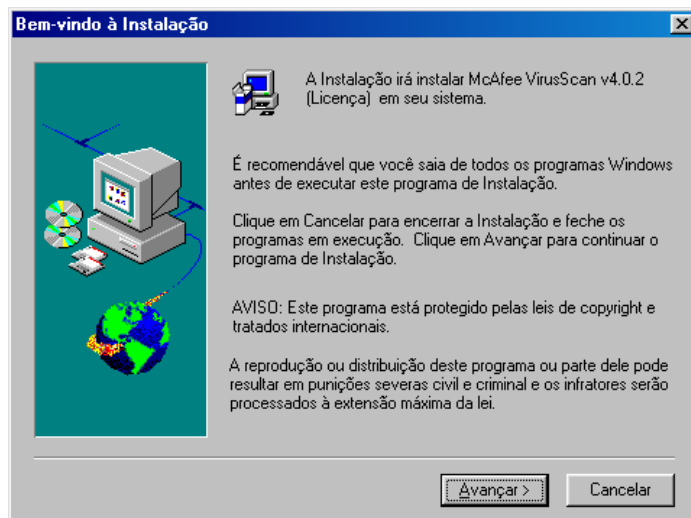
Figura 2-3. Painel do assistente Bem-vindo à configuração

3. Clique em **Avançar>** para continuar.

   O próximo painel do assistente exibe o contrato de licença do usuário final do VirusScan. Leia-o com atenção — se você instalar o VirusScan, estará aceitando a sujeição aos termos da licença.

4. Se você não concordar com os termos da licença, clique em **Não**.
   O programa de configuração será fechado imediatamente.
   Caso contrário, clique em **Sim** para continuar.

   Se esta versão do VirusScan for instalada sobre outra já existente, o programa de configuração detectará esta versão e perguntará se você deseja removê-la do seu computador. (Figura 2-4).
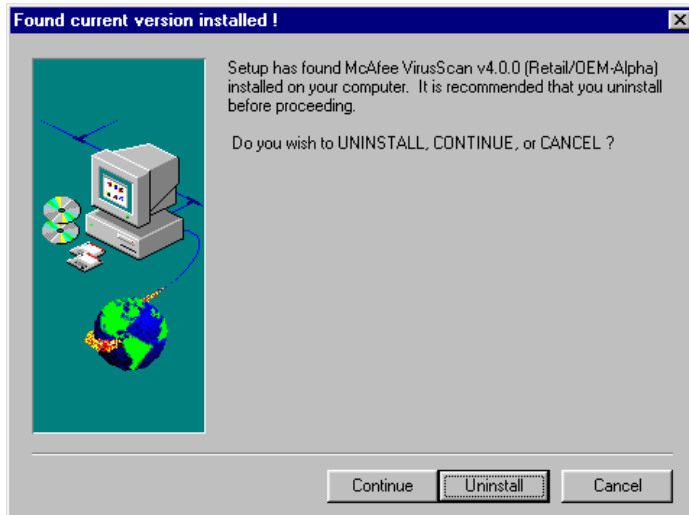
Figura 2-4. Painel Encontrada versão atual instalada

5. Para continuar, você pode:

   - Clique em **Preservar** para manter as definições escolhidas para a instalação do VirusScan existente. O programa de configuração preservará os arquivos de definições, mas removerá o restante dos arquivos de programa do VirusScan.

     NOTA: O programa de configuração manterá as definições somente para o VirusScan v4.0.1 e versões posteriores.
     Ele tentará preservar as configurações do VirusScan v3.x, mas não tentará manter as do VirusScan v2.x ou do WebScanX v3.1.6 ou anterior.

   - Clique em **Remover** para excluir a versão existente do VirusScan e todas as definições de seu computador. Quando o programa de configuração terminar de remover a versão existente do VirusScan, será exibido o painel mostrado na Figura 2-5 na página 42.
     Nesse momento, você poderá continuar na Etapa 6.

- Clique em **Sair da instalação** para interrompê-la. O programa de configuração pedirá que você confirme se deseja sair. Clique em **Sair da instalação** novamente para fechar o programa de configuração ou clique em **Continuar** para prosseguir com a instalação.

Se você continuar, o programa de configuração removerá a versão existente do VirusScan, certificando-se de ter preservado as suas definições anteriores, caso tenha sido escolhida esta opção. Quando o programa terminar de remover a versão anterior do VirusScan, será mostrado o painel Tipo de instalação (Figura 2-5).
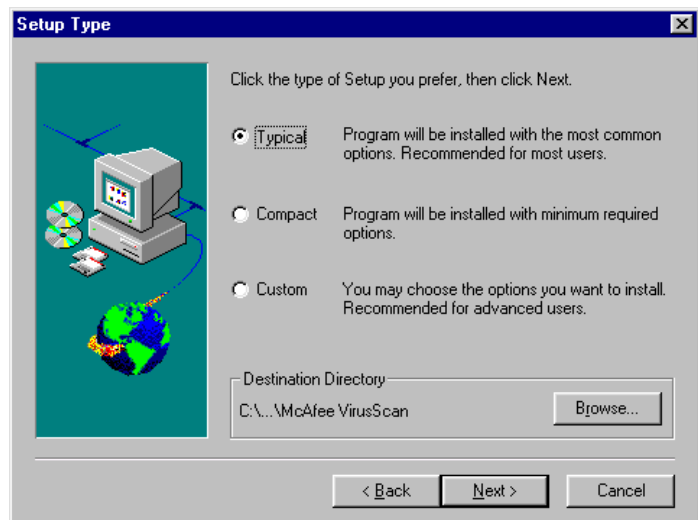
Figura 2-5. Painel Tipo de instalação

6. Selecione as definições do componente a ser instalado. Você pode escolher estas opções:

   - **Típica.** Selecione esta opção para instalar as varreduras de linha de comando do VirusScan; a varredura por solicitação do VirusScan; a varredura ao acessar do VShield; a varredura de cliente MAPI; o Programador de tarefas do VirusScan e os arquivos comuns utilizados por todos os componentes de programa. A Network Associates recomenda essa instalação para a maioria dos usuários.

   - **Compacta.** Compacta. Selecione esta opção para instalar as varreduras de linha de comando do VirusScan, a varredura ao acessar do Vshield e a varredura por solicitação do VirusScan. A Network Associates recomenda essa opção se o seu espaço livre em disco é mínimo ou caso haja outras restrições de sistema.

- **Personalizada.** Selecione esta opção para escolher quais componentes do VirusScan você deseja instalar. Como padrão, a opção Personalizada instala os mesmos componentes da instalação Típica, mas você também pode escolher instalar a Varredura do cc:Mail, uma opção de plug-in que ativa o VShield para procurar vírus na Caixa de Entrada do Lotus cc:Mail (Veja “Escolhendo opções de Detecção” na página 109 para obter mais detalhes) e o ScreenScan, um assistente de varredura que examina o seu sistema em busca de vírus quando a proteção de tela é ativada.

7. Clique em **Procurar** para localizar a pasta a ser usada para a instalação. Como padrão, o programa de configuração instala o VirusScan nesse caminho:

   C:\Program Files\Network Associates\McAfee VirusScan

8. Após escolher o conjunto de componentes a serem instalados e especificar o destino, clique em **Avançar>** para continuar.

   - **Se você escolher a instalação Típica ou um conjunto de componentes na instalação Compacta**, o programa de configuração exibirá um painel de assistente que confirma a sua escolha de componentes e o diretório de destino especificado. Como padrão, o programa de configuração procura os vírus existentes na partição do seu disco rígido e nos setores de inicialização, e na memória do computador, antes de instalar o VirusScan. Esse programa também adiciona um comando **Examinar** nos menus de atalho mostrados quando você clica com o botão direito nos objetos da área de trabalho ou no Windows Explorer.

     Se as opções mostradas refletirem as suas opções, clique em **Avançar>**. Caso contrário, clique em **<Voltar** para alterá-las. **Vá para a** Etapa 9 na página 45.

   - **Se você escolher um conjunto de componentes da instalação Personalizada**, o programa de configuração mostrará um painel de assistente contendo uma lista de componentes disponíveis para instalação (Figura 2-6 na página 44). Selecione os componentes a serem instalados e desmarque as caixas de verificação ao lado dos itens que você não deseja.

     Ao selecionar cada componente, aparece uma descrição próxima ao botão do painel. Quando você terminar as seleções, clique em **Avançar>**.
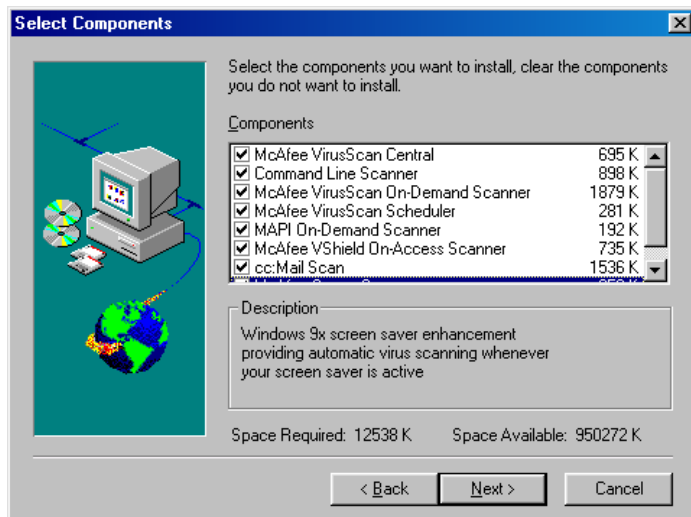
Figura 2-6. Painel Selecionar componentes

Como padrão, o programa de configuração fará o VirusScan procurar os vírus existentes na partição do seu disco rígido e nos setores de inicialização, e na memória do computador, antes de concluir a instalação. O programa de configuração também adicionará um comando Examinar nos menus de atalho mostrados quando você clica em um objeto com o botão direito na sua área de trabalho ou no Windows Explorer. Clique em **Avançar>** na parte inferior de cada um dos dois painéis seguintes para continuar.

Se você não deseja que o programa de configuração realize estas ações, desmarque as caixas de verificação que aparecerem em cada painel, em seguida clique em **Avançar>** para continuar.

Em seguida, o programa de configuração iniciará brevemente o VirusScan para examinar o disco rígido e a memória em busca de vírus antes de continuar.

9. Se o VirusScan relatar que o sistema está limpo, clique em **OK** para continuar. Se o VirusScan detectar uma infecção por vírus, saia do programa de configuração imediatamente. Veja "Se você suspeitar que há um vírus..." na página 61 para saber o que fazer a seguir.

10. O programa de configuração começará a copiar os arquivos do VirusScan para o seu computador. Ao aproximar-se da conclusão do procedimento de cópia, o programa lhe perguntará se deseja criar um Disco de emergência (Figura 2-7).
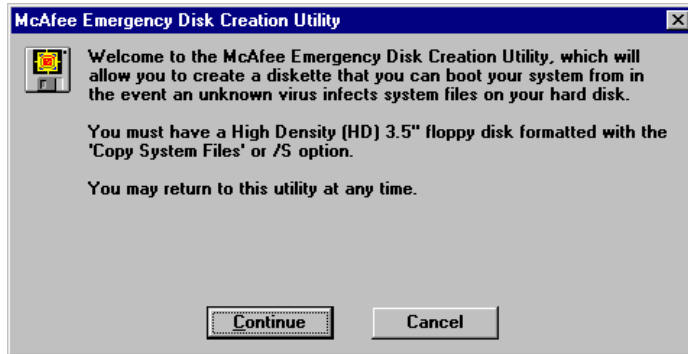
Figura 2-7. Painel do Assistente do Disco de emergência

11. Para ignorar essa etapa, clique em **Cancelar**, em seguida vá para a Etapa 16— você pode criar o Disco de emergência após a instalação. Para criá-lo agora, clique em **Avançar>**.

NOTA: A Network Associates recomenda enfaticamente que o Disco de emergência seja criado durante a instalação, mas depois que o VirusScan tiver examinado o sistema em busca de vírus. Se for detectado um vírus no seu sistema, *não* crie um Disco de emergência no computador infectado.

---

12. Aparece o próximo painel de assistente (veja a Figura 2-8). Aqui, você tem duas opções:

    - Se você tiver um disquete *livre de vírus*, *formatado* que contenha somente os arquivos de sistema DOS ou Windows, insira-o na unidade de disco. Em seguida, marque a caixa de verificação **Não formatar** , em seguida clique em **Avançar>** para continuar.

      Isto informa o assistente de Disco de emergência que deve ser copiado apenas o componente Linha de comando do VirusScan e seus arquivos de suporte para o disquete. Passe para a Etapa 13 na página 47 para continuar.
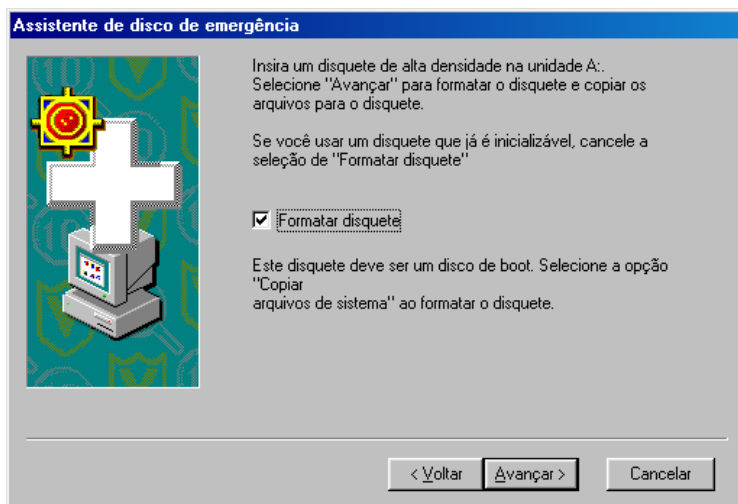
Figura 2-8. Segundo painel do Assistente de Disco de emergência

- Se você *não* tiver um disquete livre de vírus formatado com os arquivos de sistema DOS ou Windows, deverá criá-lo para poder usar o Disco de emergência a fim de iniciar o computador. Sigas estas etapas intermediárias:

    a. Insira um disquete *não formatado* na unidade de disco.

    b. Verifique se a caixa de verificação **Não formatar** está vazia.

c. Clique em **Avançar>**.

Aparece a caixa de diálogo de formatação de disco do Windows (Figura 2-9).
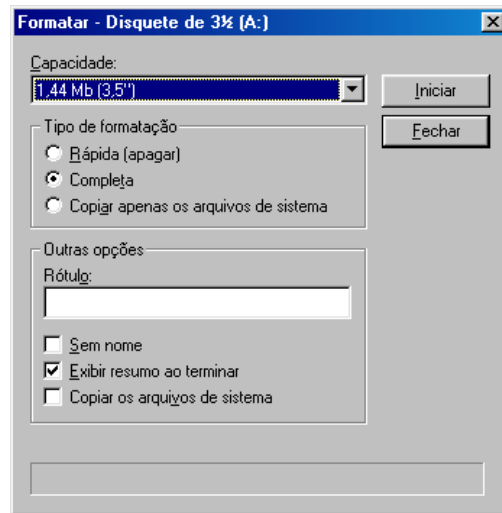
Figura 2-9. Caixa de diálogo de formatação do Windows

d. Verifique se a caixa de verificação **Completa** na área **Tipo de formatação** e a caixa de verificação **Copiar arquivos do sistema** na área **Outras opções** estão marcadas. Em seguida, clique em **Iniciar**.

O Windows formatará o disquete e copiará os arquivos de sistema necessários para iniciar o computador.

e. Clique em **Fechar** quando o Windows terminar a formatação do disco, em seguida clique em **Fechar** novamente para retornar ao painel Disco de emergência.

13. Clique em **Avançar>** para continuar. O programa de configuração examinará o seu disco recém-formatado em busca de vírus (Figura 2-10 na página 48).
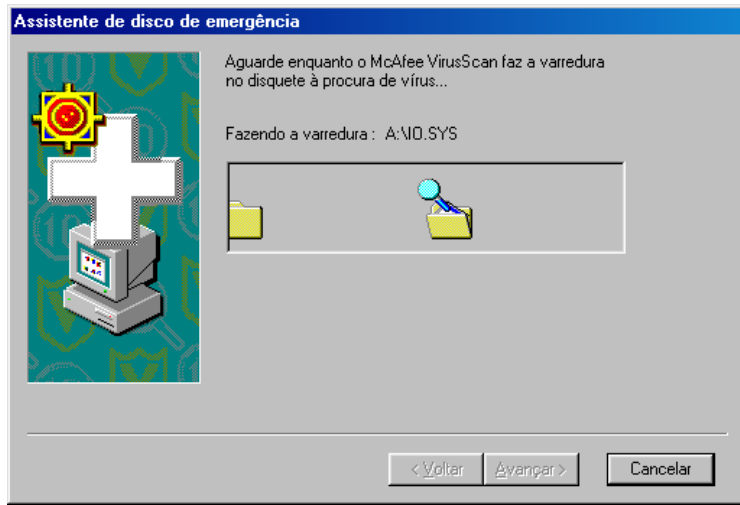
Figura 2-10. Examinando o Disco de emergência em busca de vírus

Se o VirusScan não detectar vírus durante a operação de varredura, o programa de configuração copiará imediatamente o BOOTSCAN.EXE e seus arquivos de suporte para o disquete que você criou. Se o VirusScan *detectar* um vírus, saia do programa de configuração imediatamente. Veja "Se você suspeitar que há um vírus..." na página 61 para saber o que fazer em seguida.

14. Quando o assistente termina de copiar os arquivos do Disco de emergência, ele exibe o painel final (Figura 2-11).
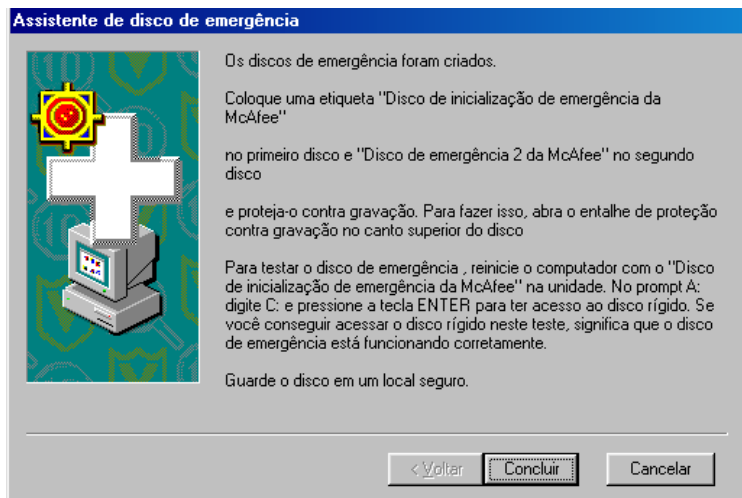
Figura 2-11. Painel final do Assistente de Disco de emergência

15. Clique em **Concluir** para retornar ao programa de configuração. Em seguida, remova o novo Disco de emergência da unidade, rotule, bloqueie e guarde-o em um local seguro.

> **NOTA:** Um disquete bloqueado apresenta dois orifícios próximos à extremidade do disquete oposta ao protetor metálico. Se você não vir essas duas aberturas, procure uma lingüeta plástica deslizante em um dos cantos do disco, em seguida deslize a lingüeta até encaixar-se em uma posição que deixe um orifício vazado.

O programa de configuração terminará de copiar os arquivos de instalação do VirusScan no seu disco rígido, em seguida apresentará uma lista com os nomes dos arquivos de sistema alterados. O programa de configuração coloca o AUTOEXEC.BAT na lista porque ele adiciona uma linha nesse arquivo, que instrui o VirusScan a executar uma operação de varredura sempre que você iniciar o computador. Esse programa também faz um backup do arquivo AUTOEXEC.BAT original e o renomeia com uma extensão diferente, caso seja necessário restaurá-lo.

16. Anote o nome de arquivo utilizado pelo programa de configuração para renomear o AUTOEXEC.BAT, para referência posterior, em seguida clique em **Avançar>** para continuar.

17. O programa de configuração pede que o computador seja reiniciado para concluir a instalação do VirusScan. Isso também assegura que o componente VShield iniciará a varredura em busca de vírus imediatamente. Se tiver outro trabalho a fazer, selecione **Não, reiniciarei meu computador posteriormente**, em seguida clique em **Concluir**. Caso contrário, selecione **Sim, desejo reiniciar meu computador agora** e clique em **Concluir** para reiniciar o sistema.

> **IMPORTANTE:** A Network Associates recomenda enfaticamente que o computador seja reinicializado imediatamente para ativar a proteção antivírus do VShield. Se você tiver feito download da cópia do VirusScan e quiser validá-la, faça o seguinte *antes* de reiniciar. Veja “Validando os seus arquivos” para saber como executar essa verificação.

Executando uma instalação “silenciosa”

Se você for um administrador de rede e deseja distribuir o VirusScan como um aplicativo de segurança antivírus padrão, poderá usar o recurso de instalação “silenciosa” do programa para configurar o VirusScan em cada nó de rede com pouca ou nenhuma interação dos usuários finais. Durante uma instalação silenciosa, o programa de configuração não exibe as janelas e painéis usuais do assistente e também não oferece opção de configuração ao usuário final. Em vez disso, você predefine essas opções e executa o programa de configuração em segundo plano em cada estação de trabalho de destino. É possível, se desejar, até mesmo instalar o VirusScan em qualquer estação de trabalho que esteja desacompanhada ou sem o conhecimento do usuário final, contanto que disponha de todos os privilégios administrativos necessários.

Uma instalação silenciosa consiste de duas etapas principais. Na primeira, você deve instalar os mesmos componentes do VirusScan no seu computador ou servidor administrativo no qual o programa de configuração deverá fazer a instalação em cada estação de trabalho de destino. Um modo especial do programa de configuração registra as opções feitas durante a instalação e preserva-as em um arquivo de configuração chamado SETUP.ISS. Em seguida, use um modo diferente do programa de configuração para instalar uma definição do VirusScan idêntica em cada sistema de destino. O programa de configuração utilizará o arquivo SETUP.ISS que você criou na primeira etapa para guiar cada instalação subseqüente a ser realizada.

Registrando as suas preferências

Para registrar as suas preferências de instalação, siga estas etapas:

1. Procure um arquivo SETUP.ISS já existente na pasta \WINDOWS do computador ou servidor de administração. Se você encontrar um arquivo com esse nome na pasta WINDOWS, renomeie ou exclua-o.

   Ao serem gravadas as preferências, o programa de configuração as salva em um novo arquivo SETUP.ISS na mesma localização.

2. Escolha **Executar** no menu **Iniciar**, na barra de tarefas do Windows.

   Aparecerá a caixa de diálogo Executar (Figura 2-12).
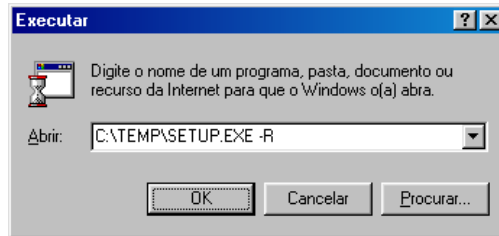
Figura 2-12. Caixa de diálogo Executar

3. Digite <X>:\SETUP.EXE -R na caixa de texto mostrada, depois clique em **OK**.

   Nessa caixa, o <X> representa a letra da sua unidade de CD-ROM ou o caminho para a pasta que contém os arquivos do VirusScan extraídos. -R informa ao programa de configuração que a sua execução deve ser no modo de “gravação”.

   NOTA: Se a origem de sua cópia do VirusScan é um CD-ROM da VirusScan Security Suite ou da Total Virus Defense CD-ROM, é necessário especificar também qual pasta contém o VirusScan para Windows 95 e Windows 98. Veja o arquivo CONTENTS.TXT incluído em qualquer uma das suites do produto para obter mais detalhes.

   Para procurar o SETUP.EXE no seu disco rígido ou no CD-ROM, clique em **Procurar**. Certifique-se de ter adicionado -R na instrução de execução, se você usar esta opção.

4. Siga as etapas de instalação descritas nas páginas 41 a 49 para escolher os componentes e as definições para as estações de trabalho de destino.

O programa de configuração anota as opções escolhidas em cada etapa e grava-as como entradas no SETUP.ISS.

IMPORTANTE: Tenha cuidado especial durante essa instalação inicial para responder a quaisquer perguntas que aparecerem nos painéis do assistente e seguir as etapas de instalação na seqüência apresentada, caso contrário a instalação silenciosa que será executada posteriormente não se realizará. Você não deve voltar atrás durante a instalação para alterar as suas definições.

Para especificar opções diferentes, é necessário reiniciar a instalação para que o programa de configuração grave as suas opções corretamente. Se você planeja instalar o VirusScan em estações de trabalho desacompanhadas, certifique-se de ter especificado opções que não necessitem da participação do usuário — não peça ao programa de configuração para criar um Disco de emergência durante a instalação, por exemplo.

A instalação também será interrompida se o VirusScan detectar um vírus no seu computador ou no servidor.

5. Quando a instalação estiver concluída, clique em **Concluir** para sair do programa de configuração.

Editando o arquivo SETUP.ISS para especificar um diretório de instalação

Se você deseja que o programa de configuração instale o VirusScan em um diretório específico, é necessário editar o arquivo SETUP.ISS, que foi criado quando você instalou o VirusScan no seu computador ou no servidor de administração. Para facilitar a administração da rede, por exemplo, talvez você prefira instalar todas as cópias do VirusScan no mesmo diretório em cada nó da rede.

O SETUP.ISS é apenas um arquivo de texto especialmente formatado, semelhante aos arquivos de configuração, como WIN.INI ou SYSTEM.INI. É possível abri-lo em qualquer editor de texto e alterar as suas entradas para que atendam às suas necessidades.

NOTA: A Network Associates recomenda que você faça somente poucas alterações no arquivo SETUP.ISS. Se você deseja ter controle completo sobre o processo de instalação ou especificar as opções de configuração para cada cópia do VirusScan previamente, é possível usar o ISeamless, uma ferramenta avançada de criação de scripts da Network Associates projetada para esse objetivo. Entre em contato com o Suporte técnico Network Associates para obter mais detalhes.

O SETUP.ISS especifica um diretório de instalação como um valor para a variável **szDir,** que pode ser encontrado em uma lista abaixo do cabeçalho **[SdSetupType-0]**. Como padrão, essa entrada é mostrada na forma abaixo:

```
[SdSetupType-0]
szDir=C:\Program Files\Network Associates\McAfee VirusScan\
Result=403
```

Para especificar um diretório de instalação diferente, substitua o caminho mostrado pelo de sua escolha. O diretório de instalação especificado aqui substituirá o diretório padrão em cada destino do sistema.

IMPORTANTE: O programa de configuração cria um único arquivo SETUP.ISS para cada produto da Network Associates, em cada plataforma. Deve ser utilizado o arquivo que corresponda ao sistema operacional que está sendo executado na estação de trabalho de destino. Você não pode, por exemplo, usar um arquivo SETUP.ISS criado durante uma instalação do VirusScan para Windows 95 para controlar outra instalação do VirusScan para Windows NT.

6. Salve o arquivo no formato de texto, em seguida saia do editor de texto.

    IMPORTANTE: A Network Associates recomenda que o arquivo SETUP.ISS criado seja utilizado para executar uma instalação de teste em uma única estação de trabalho antes de ser utilizado para distribuir o VirusScan sua rede.

Executando uma instalação silenciosa

Quando o arquivo SETUP.ISS contiver uma lista de todos os componentes e configurações desejadas para cada estação de trabalho da sua rede, você poderá replicar essas definições exatamente para cada cópia do VirusScan a ser instalada. Veja “Registrando as suas preferências” na página 50 para saber como criar o arquivo SETUP.ISS.

Você pode executar uma instalação silenciosa de várias maneiras e com diferentes níveis de interação com os usuários de rede. É possível, por exemplo, criar um script para os seus usuários que execute uma instalação silenciosa do VirusScan assim que eles se conectarem a um servidor de autenticação, sem mais nenhuma interação além da que é necessária para estabelecer a conexão. Pode ser solicitado aos usuários que executem a instalação a partir de um determinado servidor. Outras opções incluem a distribuição do VirusScan através de um aplicativo de gerenciamento de rede, como Zero Administration Client (ZAC) da Network Associates, System Management Server (SMS) da Microsoft ou de pacotes semelhantes.

Qualquer que seja o método escolhido, você deve primeiro preparar o pacote do VirusScan para instalação, em seguida executar o programa de configuração no modo silencioso.

Siga estas etapas:

1. Copie os arquivos de instalação do CD-ROM do VirusScan ou da pasta no seu computador de administração no qual estão armazenados em um diretório do VirusScan em um servidor central. Os usuários ou o aplicativo de gerenciamento de rede instalarão o VirusScan a partir deste servidor.

2. Localize o arquivo SETUP.ISS armazenado no diretório do VirusScan, no servidor central. Renomeie-o ou exclua esse arquivo.

3. Copie o arquivo SETUP.ISS, criado quando você executou a instalação gravada no seu computador de administração, no diretório do VirusScan no servidor central. O arquivo a ser copiado encontra-se no diretório WINDOWS do seu computador de administração. Veja “Registrando as suas preferências” na página 50 para saber como registrar a instalação.

   Quando essa etapa for concluída, os usuários ou o aplicativo de gerenciamento de rede podem executar o programa de configuração no modo silencioso para replicar a instalação registrada.

Para executar o programa de configuração no modo silencioso, inclua a linha `<X>:\SETUP.EXE -S` em qualquer script de conexão escrito ou em qualquer instrução para os usuários que descreva como executar o programa de configuração. Nesta linha, <X> representa o caminho para a pasta do servidor que contém os arquivos de instalação do VirusScan e o arquivo SETUP.ISS criado. -S informa ao programa de configuração que sua execução deve ser no modo silencioso. Como padrão, o programa de configuração reinicia a estação de trabalho ao concluir a instalação dos arquivos.

Se você não deseja que o programa de configuração reinicialize cada estação de trabalho de destino, é necessário editar o arquivo SETUP.ISS, criado durante a instalação registrada. Aqui, você alteraria o valor na entrada **BootOption** sob o cabeçalho **[sdFinishReboot - 0]** de seu valor atual para zero (0). Isso informa ao programa de configuração que não deve forçar a estação de trabalho de destino a reinicializar.

Como uma etapa adicional que estimule um esquema de segurança antivírus consistente em toda a rede, você pode copiar um arquivo de configuração com as opções que os usuários devem ter no diretório de instalação de cada estação de trabalho. É possível também usar proteção por senha para impedir alterações não autorizadas nas definições de configuração escolhidas. Para saber como salvar as suas definições em um arquivo de configuração, veja “Usando os menus do VirusScan” na página 155. Para saber como proteger as suas definições com uma senha, veja “Ativando a proteção por senha” na página 181.

NOTA: Para predefinir as suas opções de configuração de maneira que o VirusScan seja instalado com essas opções, use a ferramenta de criação de scripts ISeamless da Network Associates. Esse utilitário permite que você tenha total controle sobre as opções de instalação e configuração. Entre em contato com o seu representante de vendas ou com o suporte técnico da Network Associates para obter mais detalhes.

Validando os seus arquivos

A obtenção de arquivos por download ou copiá-los de outras origens externas coloca o seu computador sob risco de infecção por vírus — mesmo que o risco seja pequeno. Fazer download de software antivírus não é uma exceção. A Network Associates usa medidas de segurança rigorosas e amplas para assegurar que os produtos adquiridos e obtidos por download em seu site da web e por meio de outros serviços eletrônicos são seguros, confiáveis e livres

de infecções por vírus. Mas o software antivírus tende a atrair a atenção de desenvolvedores de programas de vírus e do tipo cavalo de Tróia, alguns dos quais acham engraçado enviar cópias de softwares comerciais infectadas posteriormente ou usar os mesmos nomes de arquivos para camuflar o seu próprio trabalho.

Você pode proteger o seu computador contra essa possibilidade ou contra a possibilidade dos seus arquivos obtidos por download serem danificados, assegurando que

- Os arquivos serão obtidos por download somente no site da web da Network Associates; e que você
- Validará os arquivos obtidos por download.

A Network Associates inclui uma cópia do VALIDATE.EXE, o seu software de validação, em cada pacote do VirusScan.

Para validar os seus arquivos, siga estas etapas:

1. Instale o VirusScan conforme a descrição em "Etapas da instalação" nas páginas 38 a 49.
2. Clique em **Iniciar** na barra de tarefas do Windows, aponte para **Programas**, em seguida escolha **Prompt do MS-DOS**.
3. Na janela mostrada, altere o prompt da linha de comando para que indique o diretório que contém os arquivos do VirusScan instalados. Se você escolher as opções de instalação padrão, os arquivos estarão neste caminho:

   C:\Program Files\Network Associates\McAfee VirusScan

   Para chegar a esse diretório, digite `cd progra~1\networ~1\mcafee~1` no prompt da linha de comando, em seguida pressione ENTER. Se o VirusScan for instalado em um diretório diferente, digite o caminho correto para esse diretório.

4. Execute o VALIDATE.EXE. Para fazê-lo, digite `validate *.*` no prompt da linha de comando.

   O VALIDATE.EXE examina todo os arquivos armazenados no seu diretório de programas do VirusScan, em seguida gera uma lista que inclui o nome do arquivo, seu tamanho em bytes, a data e hora da criação, além de dois códigos de validação em colunas separadas.

   Para usar o VALIDATE.EXE a fim de examinar arquivos individuais, basta colocar o nome do arquivo a ser verificado no prompt após `validate`, ou utilize os coringas do DOS `?` e `*` para especificar um intervalo de arquivos.

   NOTA: A Network Associates recomenda o redirecionamento da saída do VALIDATE.EXE para a impressora a fim de que você possa revê-la facilmente. Se você configurar a sua impressora para capturar a saída dos programas do MS-DOS, basta digitar `validate *.* >prn` no prompt da linha de comando.
   Para aprender a configurar a impressora para impressão a partir de programas do MS-DOS, consulte a documentação do Windows.

   Para assegurar que os seus arquivos são exatamente os mesmos que os engenheiros empacotaram na sua cópia do VirusScan, você precisa comparar os códigos de validação com os que constam na lista de validação fornecida com o programa. Essa lista é um arquivo de texto que contém os códigos de validação gerados pelos engenheiros da Network Associates com os processos de CRC (cyclical redundancy check) independentes quando eles empacotaram o VirusScan para distribuição. Esse método oferece um alto grau de segurança e impede a adulteração.

5. Para exibir a lista de empacotamento, digite `type packing.lst` no prompt da linha de comando e pressione ENTER.

   NOTA: A Network Associates recomenda novamente que você redirecione a saída do PACKING.LST para a impressora.
   Para fazê-lo, digite `type packing.lst >prn` no prompt da linha de comando.

6. Compare a saída do VALIDATE.EXE com a do PACKING.LST.
   Os tamanhos, horas e datas de criação, e os códigos de validação para cada nome de arquivo devem corresponder exatamente. Caso contrário, exclua o arquivo imediatamente — *não* abra ou examine o arquivo com outro utilitário, isso provoca risco de infecção por vírus.

   IMPORTANTE: A verificação da instalação do VirusScan com o VALIDATE.EXE não *garante* que a sua cópia esteja livre de defeitos, erros de cópia, infecções por vírus ou adulteração, mas os recursos de segurança do programa tornam extremamente improvável que alguém adultere arquivos que tenham códigos de validação corretos. Veja os arquivos LICENSE.TXT ou README.1ST incluídos na sua cópia do VirusScan para conhecer os termos da licença que rege o uso do programa.

Testando a sua instalação

Uma vez instalado, o VirusScan está pronto para examinar o sistema em busca de arquivos infectados. Você pode testar se a instalação está correta e se o programa examinou a ocorrência de vírus adequadamente, implementando um teste desenvolvido pelo European Institute of Computer Anti-virus Research (EICAR), uma coalizão de fornecedores de programas antivírus, como um método para ser usado pelos clientes a fim de testar qualquer instalação de software antivírus.

Para testar a instalação, siga estas etapas:

1. Abra um editor de texto padrão do Windows, como o Bloco de Notas, em seguida digite:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
TEST-FILE!$H+H*
```

   NOTA: A linha mostrada acima deve aparecer como *única* na janela do editor de texto. Se você estiver lendo esse manual no computador, poderá copiá-la diretamente do arquivo do Acrobat para o Bloco de Notas.

2. Salve esse arquivo com o nome EICAR.COM. O tamanho do arquivo deverá ser 69 ou 70 bytes.

3. Inicie o VirusScan e deixe-o examinar o diretório que contém o EICAR.COM. Quando o VirusScan examinar esse arquivo, relatará que encontrou o vírus EICAR-STANDARD-AV-TEST-FILE.

IMPORTANTE: Esse arquivo *não é um vírus* — e não poderá espalhar-se e infectar outros arquivos ou danificar o seu sistema de qualquer outro modo. Exclua o arquivo ao concluir o teste da instalação para evitar alarmar outros usuários.

Removendo infecções Do seu sistema

3

Se você suspeitar que há um vírus...

Antes de tudo, não entre em pânico! Embora estejam longe de serem inofensivos, a *maioria* dos vírus que infectam a sua máquina não destroem os dados, nem pregam peças ou inutilizam o seu computador. Mesmo se comparados aos vírus raros que trazem uma carga destrutiva, normalmente, produzem os seus efeitos malignos em resposta a um evento acionador. Na maioria dos casos, a menos que você constate a evidência de já foi ativada uma carga viral, terá tempo para tratar da infecção adequadamente. A presença desses pequenos pedaços de código de computador indesejados podem, contudo, interferir na operação normal da máquina, consumir recursos do sistema e gerar outros efeitos nocivos, por isso, leve-os a sério e assegure a sua remoção quando forem encontrados.

É preciso não esquecer também que um comportamento estranho do computador, falhas de sistema não explicadas ou outros eventos imprevisíveis podem ter causas diferentes da infecção por vírus. Se você acredita que há um vírus no seu computador devido a ocorrências como estas, a varredura para buscar vírus pode não produzir os efeitos esperados, mas ajudará a eliminar uma causa potencial dos problemas de seu computador.

A melhor atitude a tomar é instalar o VirusScan e realizar um exame imediato e completo do sistema.

Como se auto-instala, o VirusScan examinará a memória do seu computador e os setores de inicialização do disco rígido para verificar se poderá copiar os seus arquivos com segurança para o disco rígido sem risco de infectá-los. Se, durante a instalação, o VirusScan relatar que o sistema parece estar livre de vírus, continue a instalação, em seguida execute um exame completo do sistema assim que reiniciar o computador — os vírus que infectam arquivos, que não são carregados na memória do computador ou que se ocultam nos blocos de inicialização do disco rígido, ainda podem estar escondidos em algum lugar do seu sistema. Veja o Capítulo 2, “Instalando o McAfee VirusScan,” para saber como é feita a varredura em busca de vírus durante a instalação. Veja Capítulo 5, “Usando o McAfee VirusScan,” para saber como executar uma varredura completa do sistema.

Se o VirusScan detectar um vírus durante o programa de configuração, você precisará removê-lo do sistema antes de instalar o programa. Para aprender a fazê-lo, siga as etapas que começam na pagina 62.

IMPORTANTE: Para assegurar máxima segurança, você deve seguir estas mesmas etapas se o VirusScan detectar um vírus, posteriormente, na memória do seu computador, após a instalação do programa.

Se o VirusScan encontrar uma infecção durante a instalação, siga estas etapas cuidadosamente:

1. Saia do programa de instalação imediatamente, em seguida feche o computador.

   Certifique-se de ter desligado completamente a energia do sistema. *Não* pressione CTRL+ALT+DEL ou o botão Reset do computador para reiniciar o sistema — alguns vírus podem permanecer intactos durante esse tipo de inicialização a quente.

2. Se a sua cópia do VirusScan contiver um Disco de emergência, insira-o na unidade de disco.

   NOTA: Se a sua cópia do VirusScan não contiver um Disco de emergência da McAfee ou se você não o encontrou, deverá criar um novo disco em um computador *não infectado*. Procure um computador que esteja sem vírus, depois siga as etapas descritas em “Criando um Disco de emergência” na página 64.

3. Inicie novamente o computador.

   O Disco de emergência dará partida no computador e iniciará imediatamente o BOOTSCAN.EXE, uma varredura de linha de comando com um objetivo especial. O programa lhe perguntará se você desligou a energia do computador antes de iniciá-lo com o Disco de emergência. Se a resposta for positiva, pressione S no seu teclado, em seguida continue na Etapa 4. Caso contrário, pressione N, em seguida desligue completamente o computador e recomece.

   Uma vez iniciado, o BootScan relatará o seu andamento durante o exame do sistema e tentará remover códigos de vírus dos arquivos infectados que encontrar. Após o término da operação de varredura, serão mostrados os resultados finais: quantos arquivos foram examinados, quantos arquivos infectados foram encontrados, se o vírus foi encontrado na memória ou nos blocos de inicialização do disco rígido e outras informações.

4. Quando o BootScan termina o exame do sistema, você pode:

   - **Voltar a trabalhar com o computador.** Se o BootScan não tiver encontrado um vírus ou se tiver limpado os arquivos infectados que encontrou, remova o Disco de emergência da unidade, em seguida, reinicie o computador normalmente. Se você planejou instalar o VirusScan no seu computador, mas parou quando o programa de instalação encontrou uma infecção, não poderá continuar agora com a instalação.

   - **Tente você mesmo limpar ou excluir os arquivos infectados.** Se o BootScan encontrar um vírus mas não puder removê-lo, ele identificará os arquivos infectados e lhe informará que não pode limpá-los ou que não dispõe no momento de um removedor para esse vírus.

     Como uma próxima etapa, você pode:

     – **Localizar e excluir os arquivos infectados.** Será necessário restaurar os arquivos excluídos a partir do backup. Certifique-se de ter verificado os arquivos de backup em busca de infecções.

     – **Tente você mesmo remover a infecção.** A Network Associates fornece informações e sugestões na Biblioteca de informações sobre vírus que podem ajudá-lo a remover um vírus de um arquivo infectado. Para ver essas informações, inicie o seu aplicativo de navegação na web preferido, em seguida digite o seguinte endereço da web:

       http://www.nai.com/vinfo/<número do documento>.asp

       Nesse endereço, <número do documento> representa um documento técnico da Biblioteca de informações sobre vírus. Substitua <número do documento> por um destes números:

       0013 0319 0322 0323 0327 1145

       NOTA: Os números dos documentos podem mudar. Veja o sumário da Biblioteca de informações sobre vírus online para obter dados atualizados.

Criando um Disco de emergência

Se você não encontrar a cópia do seu Disco de emergência que acompanha o VirusScan ou se obteve por download a sua cópia do programa em um dos serviços eletrônicos da Network Associates, precisará criá-lo.

ATENÇÃO: Se o VirusScan detectar um vírus durante a tentativa de se auto-instalar no seu computador, você deverá instalá-lo em um computador *não infectado*, em seguida crie um Disco de emergência nesse sistema. Em seguida, é possível iniciar o sistema infectado com o Disco de emergência, remover o vírus da infecção e depois instalar o VirusScan neste sistema. Verifique se retirou a cópia do VirusScan do primeiro sistema a menos que a sua licença permita a instalação de diversas cópias do programa.

Para criar um Disco de emergência com o assistente de criação de Disco de emergência do VirusScan, siga estas etapas:

1. Insira um disquete em branco, *não formatado de* 1,44MB na unidade.

2. Clique em **Iniciar** na barra de tarefas do Windows, aponte para **Programas**, em seguida para **McAfee VirusScan**. Depois, escolha **Criar Disco de emergência**.

   Aparecerá o primeiro painel do assistente de Disco de emergência (Figura 3-1).
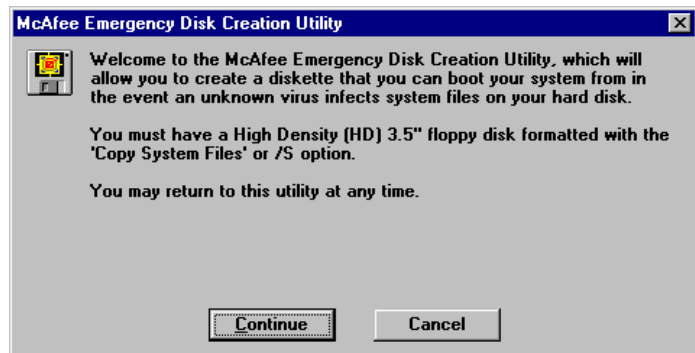
Figura 3-1. Painel Assistente de Disco de emergência

3. Clique em **Avançar>** para exibir o próximo painel do assistente (Figura 3-2). Aqui, há duas opções:

- Se você tem um disquete *formatado e sem vírus* que contenha apenas os arquivos de sistema do DOS ou do Windows, insira-o na unidade de disco. Em seguida, marque a caixa de verificação **Não formatar** em seguida, clique em **Avançar>** para continuar.

  Este procedimento informa ao assistente de Disco de emergência para copiar o componente Linha de comando do VirusScan e seus arquivos de suporte para o disquete. Passe para a Etapa 5 na página 67 para continuar.
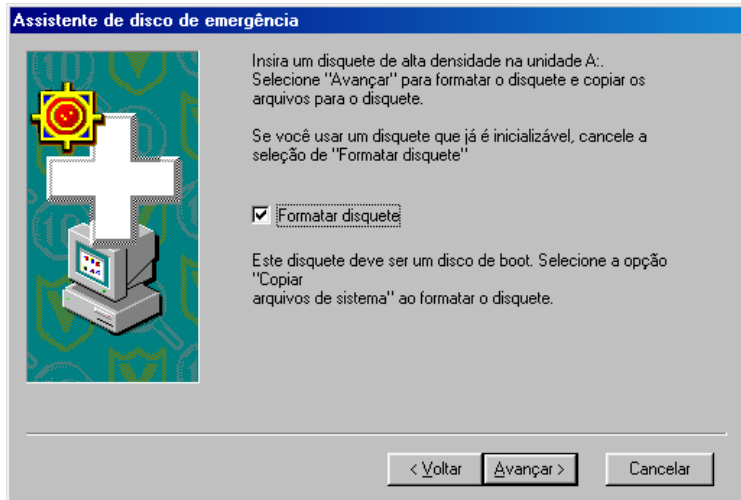
Figura 3-2. Segundo painel do Assistente de Disco de emergência

- Se você *não* tem um disquete formatado e sem vírus com os arquivos de sistema do DOS ou Windows, deve criá-lo para usar o Disco de emergência a fim de iniciar o computador.

  Siga estas etapas intermediárias:

  a. Insira um disquete *não formatado* na unidade de disco.

  b. Verifique se a caixa de verificação **Não formatar** está desmarcada.

c. Clique em **Avançar>**.

Aparece a caixa de formatação de disco do Windows (Figura 3-3).
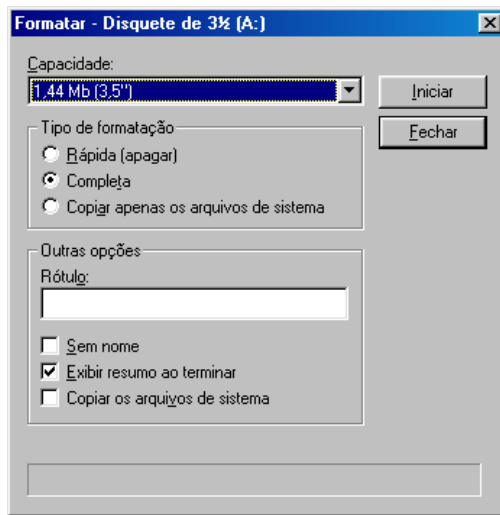
Figura 3-3. Caixa de diálogo de formatação do Windows

d. Verifique se a caixa de verificação **Completa** na área **Tipo de formatação** e a caixa de verificação **Copiar arquivos do sistema** na área **Outras opções** estão ambas marcadas. Em seguida, clique em **Iniciar**.

O Windows formatará o seu disquete e copiará os arquivos de sistema necessários para iniciar o computador.

e. Clique em **Fechar** quando o Windows terminar de formatar o seu disco, em seguida clique em **Fechar** novamente para retornar ao painel do assistente de Disco de emergência.

4. Clique em **Avançar>** para continuar. Isto informa ao assistente de Disco de emergência para copiar o componente Linha de comando do VirusScan e seus arquivos de suporte para o disquete de inicialização recém-criado.

5. Quando o assistente terminar de criar o Disco de emergência, clique em **Concluir** para retornar ao programa de configuração. Rotule o novo Disco de emergência, bloqueie e guarde-o em lugar seguro.

NOTA: Um disquete bloqueado apresenta dois orifícios próximos à extremidade do disquete oposta ao protetor metálico. Se você não vir essas duas aberturas, procure uma lingüeta deslizante de plástico em um dos cantos do disco, em seguida deslize-a até encaixar-se em uma posição que deixe um orifício vazado. Como nenhum software pode salvar em um disquete bloqueado, os vírus não poderão infectar os arquivos nele instalados.

Criando um Disco de emergência sem o utilitário

Se você não puder usar o utilitário de criação de Disco de emergência porque ainda não instalou o VirusScan ou porque esse programa detectou um vírus durante a instalação, é possível criar um Disco de emergência sem o utilitário. Siga estas etapas:

ATENÇÃO: Se o VirusScan detectar um vírus ao tentar instalar-se no seu computador, crie o seu Disco de emergência em um computador *não infectado*.

1. Abra a janela Prompt do MS-DOS ou faça uma reinicialização no computador no modo DOS. Para aprender a fazê-lo, consulte a documentação do Windows.

2. Insira um disquete em branco, *não formatado de* 1,44MB na unidade.

3. Digite este comando no prompt do MS-DOS:

   ```
   format <unidade de disco>: /s/u/v
   ```

   Substitua a letra da unidade de disco por aquela de seu disquete em `<unidade de disco>` no comando mostrado. Em seguida, pressione **ENTER.** Este procedimento instrui o sistema a formatar o disquete inserido, sobrescrever qualquer informação nele contida, copiar os arquivos de sistema do DOS nesse disquete e fazer com que o prompt lhe peça para digitar um rótulo de volume.

4. Quando o prompt do DOS lhe solicitar um rótulo de volume, digite um nome que contenha até 11 caracteres que diferenciem esse disquete dos demais.

5. Se o VirusScan foi instalado em seu computador e no diretório de programas padrão, altere para o diretório correto digitando este comando no prompt do MS-DOS:

   ```
   cd\progra~1\networ~1\mcafee~1
   ```

   Se o VirusScan não estiver instalado, altere o diretório para o que contém os arquivos do VirusScan que você extraiu, ou para o diretório VirusScan na unidade de CD-ROM.

6. Digite os comandos relacionados abaixo no prompt do MS-DOS para copiar os arquivos corretos no Disco de emergência. Substitua a letra da unidade de disco pela de sua unidade em `<unidade de disco>` nos comandos mostrados:

   ```
   copy bootscan.exe <unidade de disco>:

   copy scan.dat <unidade de disco>:

   copy names.dat <unidade de disco>:

   copy clean.dat <unidade de disco>:

   copy license.dat <unidade de disco>:

   copy messages.dat <unidade de disco>:

   copy edwiz16.exe <unidade de disco>:
   ```

7. Copie no Disco de emergência qualquer outro utilitário do DOS necessário para iniciar o seu computador, depure o software de sistema, gerencie a memória expandida ou estendida ou execute outras tarefas na inicialização. Se você usar um utilitário de compactação de disco, verifique se copiou os drivers necessários para descompactar os arquivos.

8. Ao terminar a cópia dos arquivos no Disco de emergência, rotule, bloqueie e guarde-o em lugar seguro.

NOTA: Um disquete bloqueado apresenta dois orifícios próximos à extremidade do disquete oposta ao protetor metálico. Se você não vir essas duas aberturas, procure uma lingüeta deslizante de plástico em um dos cantos do disco, em seguida deslize-a até encaixar-se em uma posição que deixe um orifício vazado. Como nenhum software pode salvar em um disquete bloqueado, os vírus não poderão infectar os arquivos nele instalados.

Reagindo a vírus ou softwares destrutivos

Como o VirusScan consiste de diversos programas de componentes, cada um deles pode estar ativo de uma vez, as suas ações possíveis a uma infecção por vírus ou a outro software destrutivo dependerão de qual programa detectou o objeto nocivo, de como o programa será configurado para atuar e de outras circunstâncias. As seções abaixo fornecem uma visão geral das ações padrão disponíveis para cada componente de programa. Para conhecer as outras ações possíveis, veja o capítulo que trata de cada componente em detalhe.

Reagindo quando o VShield detecta um software destrutivo

O VShield consiste de quatro módulos relacionados que oferecem uma proteção de varredura de segundo plano contínua contra vírus, objetos Java e ActiveX nocivos e sites da web perigosos. Um quinto módulo controla as configurações de segurança para os outros quatro. Você pode configurar e ativar cada módulo separadamente ou usá-los juntos para fornecer uma máxima proteção. Veja Capítulo 4, “Usando o VShield,” para conhecer as opções de configuração de cada módulo. Como cada módulo detecta diferentes objetos ou examina pontos de entrada de vírus distintos, cada um deles apresenta um conjunto diferente de ações padrão.

Módulo Varredura do Sistema

Como padrão, este módulo procura vírus sempre que você executa, copia, cria ou renomeia qualquer arquivo no seu sistema, ou quando lê em um disquete. Por causa disso, a Varredura do Sistema pode servir como um backup no caso de qualquer outro módulo do VShield não detectar um vírus que pode estar contido em um download, por exemplo, de um aplicativo de cliente FTP. Na sua configuração inicial, quando o módulo encontra um vírus durante qualquer uma dessas operações, ele impedirá que você abra, salve ou copie o arquivo infectado e lhe perguntará o que será feito contra o vírus (veja a Figura 3-4 na página 70).

As ações que podem ser vistas nesta caixa de diálogo pertencem às opções padrão ou àquelas que você fez na página Ações do módulo Varredura do Sistema. Veja “Escolhendo opções de Ação” na página 98 para saber como escolher quais opções aparecem aqui.
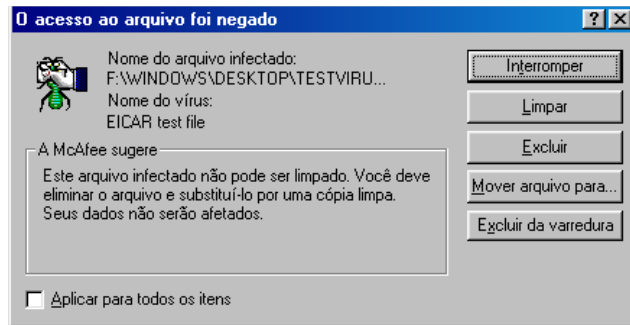
Figura 3-4. Opções de ação iniciais da Varredura do Sistema

Se você tiver marcado a caixa de verificação **Continuar acesso** na página Ações do módulo, verá um aviso que ocupa a tela inteira e oferece opções de ação (Figura 3-5).
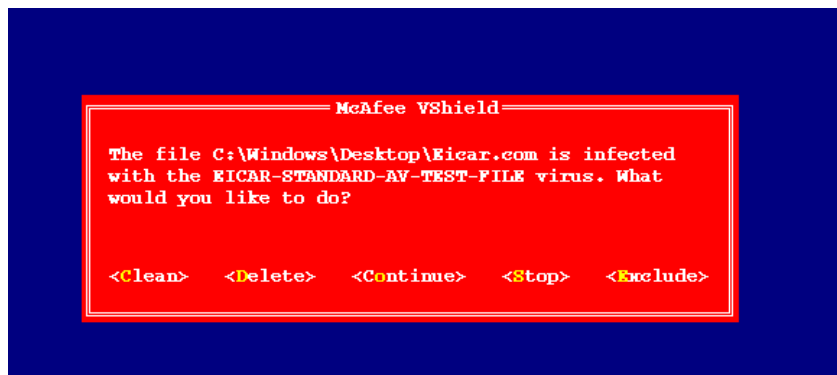
Figura 3-5. Opções de ação da Varredura do Sistema

Para realizar uma das ações da lista, clique em um botão na caixa de diálogo ou digite a letra destacada em amarelo, quando aparecer o aviso que ocupa a tela inteira. Se você quiser aplicar a mesma ação a todos os arquivos infectados que o VShield encontrar durante essa operação de varredura, marque a caixa de verificação **Aplicar a todos os itens** na caixa de diálogo. Estas são as opções:

- **Limpar o arquivo.** Clique em **Limpar** na caixa de diálogo ou digite L quando você vir o aviso que ocupa a tela inteira, para informar ao VShield que tente remover o código de vírus do arquivo infectado. Se o VShield for bem-sucedido, irá restaurar o arquivo ao seu estado original.

Se não puder limpar o arquivo — porque não tem um removedor ou o vírus danificou o arquivo e não há reparos a fazer — o resultado será anotado no arquivo de registro e não realizará outra ação. Na maioria dos casos, você deve excluir esses arquivos e restaurá-los a partir de backups.

- **Excluir o arquivo.** Clique em **Excluir** na caixa de diálogo ou digite E quando você vir o aviso que ocupa a tela inteira para informar ao VShield que exclua o arquivo infectado imediatamente. Como padrão, o VShield anotará o nome desse arquivo no arquivo de registro para que você tenha um registro de quais arquivos estão indicados como infectados. Em seguida, é possível restaurar os arquivos excluídos a partir de cópias de backup.

- **Mover o arquivo para uma localização diferente.** Clique em **Mover arquivo para** na caixa de diálogo. Este procedimento abre uma janela de navegação que pode ser utilizada para procurar a pasta de quarentena ou outra que você queira usar para isolar os arquivos infectados. Depois que a pasta é selecionada, o VShield move o arquivo infectado para essa localização imediatamente.

- **Continuar trabalhando.** Digite O quando você vir o aviso que ocupa a tela inteira para informar ao VShield que lhe permita continuar a trabalhar com o arquivo e não atuar de qualquer outra maneira. Normalmente, você usaria essa opção para ignorar arquivos que você já sabe que não contêm vírus. Se a opção de relatório estiver ativada, o VShield anotará cada ocorrência no seu arquivo de registro.

- **Parar a operação de varredura.** Clique em **Parar** na caixa de diálogo ou digite S quando você vir o aviso que ocupa a tela inteira para informar ao VShield que negue qualquer acesso ao arquivo, mas não atue de qualquer outra maneira. A negativa de acesso ao arquivo impede que você o abra, salve ou renomeie. Para continuar, clique em **OK**. Se a opção de relatório estiver ativada, o VShield anotará cada ocorrência no seu arquivo de registro.

- **Ignorar o arquivo nas operações de varredura.** Clique em **Ignorar** na caixa de diálogo ou digite I quando você vir o aviso que ocupa a tela inteira para informar ao VShield que ignore esse arquivo nas próximas operações de varredura. Normalmente, você usaria essa opção para ignorar arquivos que você já sabe que não contêm vírus.

Módulo Varredura de Correio Eletrônico

Este módulo procura vírus em mensagens de correio eletrônico recebidas via sistemas de correio eletrônico empresariais, como cc:Mail e Microsoft Exchange. Na sua configuração inicial, o módulo solicitará a escolha de uma ação entre três opções ao detectar um vírus (Figura 3-6). Uma quarta opção apresenta informações adicionais.

Figura 3-6. Opções de ação do módulo Varredura de Correio Eletrônico

Clique no botão que corresponde à ação desejada. Estas são as opções:

- **Continuar.** Clique nesta opção para que o VShield não atue e continue a varredura. O VShield continuará até encontrar outro vírus no seu sistema ou até o final da operação de varredura. Normalmente, essa opção seria usada para ignorar arquivos que você já sabe que não contêm vírus, ou se planeja afastar-se do computador durante um longo período. O VShield anotará cada ocorrência no arquivo de registro.
- **Excluir.** Clique nesta opção para que o VShield exclua o arquivo de anexo infectado da mensagem de correio eletrônico recebida. Como padrão, o VShield anota o nome do anexo no arquivo de registro.
- **Mover.** Clique nesta opção para que o VShield crie um diretório de quarentena onde encontrou o vírus, em seguida, mova o arquivo infectado para esse local. Se você usar o Microsoft Exchange, Microsoft Outlook ou outros clientes de correio MAPI, por exemplo, o diretório de quarentena aparecerá como uma pasta chamada INFECTADO, na sua caixa de correio, no servidor de correio. Se for utilizado um cliente de correio POP-3 ou semelhante, a pasta de quarentena aparecerá no nível raiz do seu disco rígido assim que você fizer download de um arquivo infectado.
- **Informações.** Clique nesta opção para conectar-se à Biblioteca de informações sobre vírus da Network Associates. Com esta opção, nenhuma ação será realizada sobre o vírus detectado pelo VShield. Veja “Exibindo informações sobre o arquivo e o vírus” na página 79 para obter mais detalhes.

Uma vez escolhida a ação, o VShield irá implementá-la e adicionará um aviso na parte superior da mensagem de correio eletrônico que contém o anexo infectado. Esse aviso fornece o nome do arquivo de anexo infectado, identifica o nome do vírus e descreve a ação desencadeada pelo VShield.

Módulo Varredura de Download

Esse módulo procura vírus em mensagens de correio eletrônico recebidas via Internet através de um navegador da Web ou de programas de clientes de correio eletrônico como Eudora Light, Netscape Mail, Outlook Express e outros. Ele *não* detecta os arquivos obtidos por download com os aplicativos de clientes FTP, aplicativos de terminais ou através de canais semelhantes. Na sua configuração inicial, o módulo solicitará a escolha de uma ação entre três opções ao detectar um vírus (Figura 3-7). Uma quarta opção apresenta informações adicionais.

Figura 3-7. Opções de ação da Varredura de Download

Clique no botão que corresponde à ação desejada. Estas são as opções:

- **Continuar.** Clique nesta opção para que o VShield não atue e continue a varredura. O VShield prosseguirá até encontrar outro vírus no seu sistema ou terminar a operação de varredura. Normalmente, essa opção seria usada para ignorar arquivos que você já sabe que não contêm vírus ou se planeja afastar-se do computador ao fazer download de correio eletrônico ou de outros arquivos. O VShield anotará cada ocorrência no arquivo de registro.

- **Excluir.** Clique nesta opção para que o VShield exclua o arquivo infectado ou o anexo de correio eletrônico recebido. Como padrão, o VShield anota o nome do arquivo infectado no arquivo de registro.

- **Mover.** Clique nesta opção para que o VShield crie um diretório de quarentena onde encontrou o vírus, em seguida, mova o arquivo infectado para esse local. Se você usar um cliente POP-3 ou SMTP de correio eletrônico, a pasta de quarentena aparecerá com o nome INFECTADO no nível raiz do seu disco rígido assim que você fizer download de um arquivo infectado.
- **Informações.** Clique nesta opção para conectar-se à Biblioteca de informações sobre vírus da Network Associates. Esta opção não realiza nenhuma ação contra o vírus. Veja "Exibindo informações sobre o arquivo e o vírus" na página 79 para obter mais detalhes.

Uma vez escolhida a ação, o VShield irá implementá-la e adicionará um aviso na parte superior da mensagem de correio eletrônico que contém o anexo infectado. Esse aviso fornece o nome do arquivo de anexo infectado, identifica o nome do vírus e descreve a ação desencadeada pelo VShield.

Módulo Filtro de Internet

Esse módulo procura classes Java e controles ActiveX hostis quando você visita um site da web ou faz download de arquivos na Internet. Esse módulo também pode ser usado para bloquear a conexão do seu navegador aos sites da Internet perigosos. Na sua configuração inicial, o módulo precisa saber, no caso de encontrar um objeto potencialmente nocivo, se você deseja **Negar** ao objeto acesso ao sistema ou se deseja **Continuar** e permitir o acesso do objeto. Estas opções serão apresentadas quando você tentar conectar-se a um site da web potencialmente perigoso (Figura 3-8).
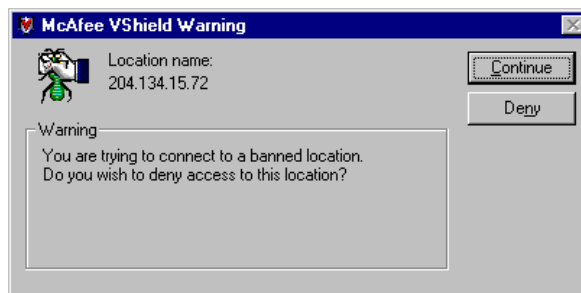
Figura 3-8. Opções de ação do Filtro de Internet

Reagindo quando o VirusScan detecta um vírus

Na primeira vez que você instala o VirusScan e inicia uma operação de varredura, o programa examinará todos os arquivos na unidade C: suscetíveis a infecção por vírus. Esse procedimento oferece um nível básico de proteção que pode ser estendido, configurando o VirusScan para atender as suas necessidades. Na sua configuração inicial, o programa lhe solicitará uma ação quando detectar um vírus (Figura 3-9 na página 75).
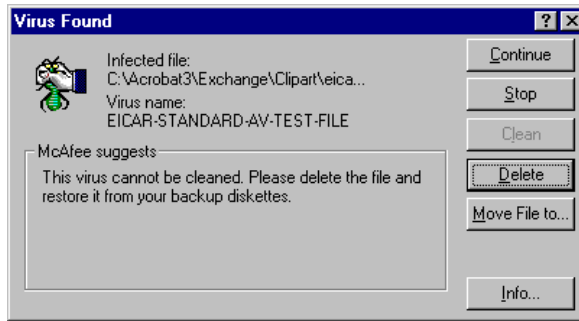
Figura 3-9. Opções de ação do VirusScan

Para reagir à infecção, clique em um dos botões mostrados. Você pode instruir o VirusScan para:

- **Continuar.** Clique nesta opção para continuar a operação de varredura e fazer com que o VirusScan coloque cada arquivo infectado na lista, na parte inferior da sua janela principal (Figura 3-10) e insira cada detecção no arquivo de registro, mas não atue de qualquer outra maneira contra o vírus. Quando o VirusScan termina o exame do sistema, você pode clicar com o botão direito do mouse em cada arquivo contido na lista, na janela principal, e escolher uma ação individual no menu de atalho mostrado.
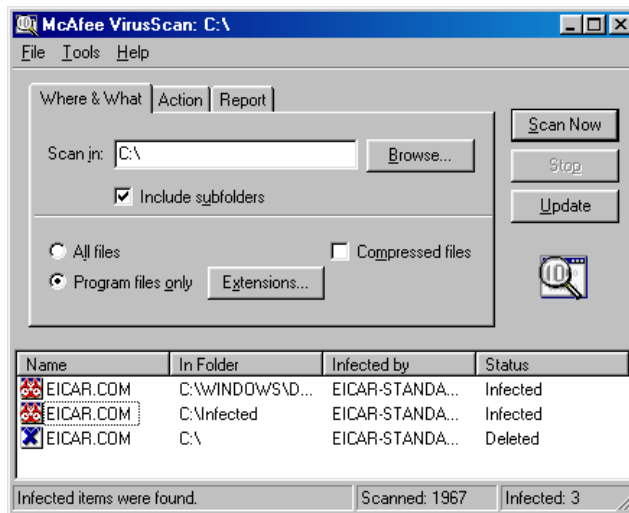
Figura 3-10. Janela principal do VirusScan

- **Parar.** Clique nesta opção se quiser parar a operação de varredura imediatamente. O VirusScan fará uma lista dos arquivos infectados já encontrados na parte inferior de sua janela principal (Figura 3-10) e registrará cada detecção no arquivo de registro, mas não atuará de qualquer outra maneira contra o vírus. Clique com o botão direito em cada arquivo infectado contido na lista na janela principal e escolha uma ação individual no menu de atalho mostrado.

- **Limpar.** Clique nesta opção para que o VirusScan tente remover o código de vírus do arquivo infectado. Se não puder limpá-lo — porque não tem um removedor ou o vírus danificou o arquivo e não há mais reparo a fazer — irá registrar a ocorrência no arquivo de registro e sugerir ações alternativas. No exemplo mostrado na Figura 3-9, o VirusScan não limpou o Vírus de Teste da Eicar — um falso vírus programado especificamente para testar se o software antivírus foi instalado corretamente. Aqui, **Limpar** não é uma opção de ação disponível. Na maioria dos casos, você deve excluir esses arquivos e restaurá-los a partir de backups.

- **Excluir.** Clique nesta opção para excluir o arquivo do sistema imediatamente. Como padrão, o VirusScan inclui o nome do arquivo infectado no registro para que você possa restaurá-lo a partir de uma cópia de backup.

- **Mover arquivo para.** Clique nesta opção para abrir uma caixa de diálogo que pode ser utilizada para procurar a sua pasta de quarentena ou uma outra pasta adequada. Uma vez encontrada a pasta correta, clique em **OK** para transferir o arquivo para essa localização.

- **Informações.** Clique nesta opção para conectar-se à Biblioteca de informações sobre vírus da Network Associates. Essa opção não atua contra o vírus detectado pelo VirusScan. Veja “Exibindo informações sobre o arquivo e o vírus” na página 79 para obter mais detalhes.

Reagindo quando a Varredura de Correio Eletrônico detecta um vírus

O componente de programa Varredura de Correio Eletrônico do VirusScan permite examinar a entrada de mensagens de correio eletrônico do Microsoft Exchange ou Microsoft Outlook em busca de vírus quando você quiser. Esse componente pode ser iniciado no cliente de correio eletrônico e usado para complementar a varredura contínua de correio eletrônico, em segundo plano, do VShield. A Varredura de Correio Eletrônico também oferece a possibilidade de limpar anexos de arquivos infectados ou parar a operação de varredura, um recurso que complementa a monitoração contínua do VShield. Na configuração inicial, a Varredura de Correio Eletrônico lhe solicitará uma ação quando encontrar um vírus (Figura 3-11 na página 77).
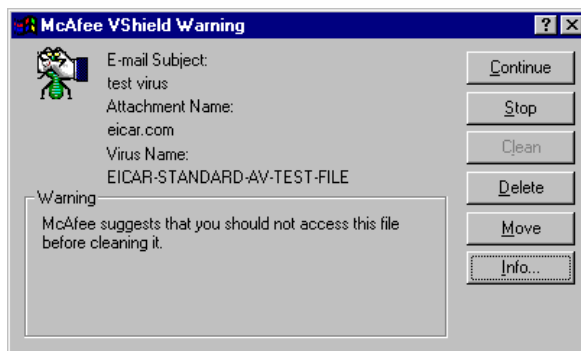
Figura 3-11. Opções de ação da Varredura de Correio Eletrônico

Para reagir à infecção, clique em um dos botões mostrados. Você pode instruir a Varredura de Correio Eletrônico a:

- **Continuar.** A Varredura de Correio de Eletrônico continua a operação de varredura, inclui na lista cada arquivo infectado encontrado, na parte inferior da sua janela principal (Figura 3-12 na página 78), e registra cada detecção no arquivo de registro, mas não realizará nenhuma outra ação contra o vírus. A Varredura de Correio Eletrônico continuará até encontrar outro vírus ou terminar a operação de varredura. Depois que esse componente termina de examinar o sistema, você pode clicar com o botão direito do mouse em cada arquivo da lista na janela principal e, em seguida, escolher uma ação individual no menu de atalho mostrado.

- **Parar.** A Varredura de Correio Eletrônico pára a operação de varredura imediatamente. Esse componente faz uma lista dos arquivos infectados que já tenham sido encontrados na parte inferior da sua janela principal (Figura 3-12 na página 78) e registra cada detecção no arquivo de registro, mas não atuará para reagir ao vírus. Clique com o botão direito em cada arquivo infectado contido na lista na janela principal e escolha uma ação individual no menu de atalho mostrado.
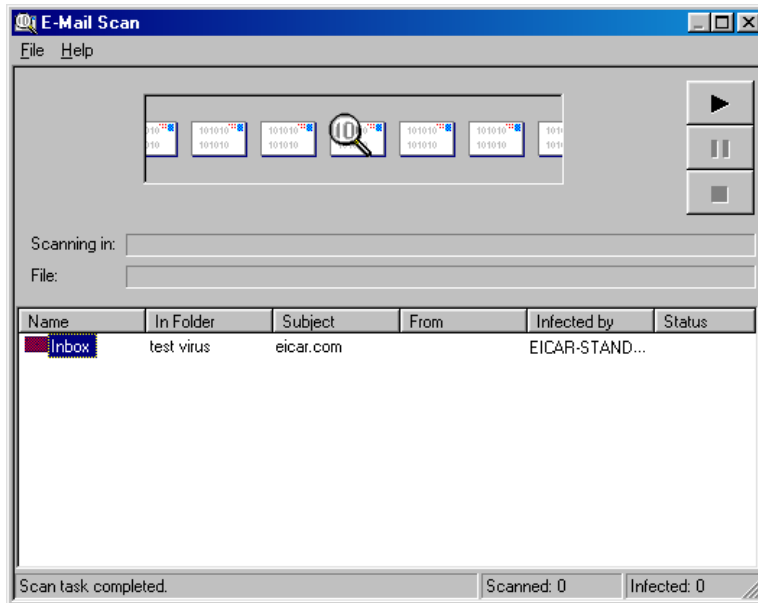
Figura 3-12. Janela Varredura de Correio Eletrônico

- **Limpar.** A Varredura de Correio Eletrônico tentará remover o código do vírus do arquivo infectado. Se não puder limpá-lo — porque não tem um removedor ou o vírus danificou o arquivo e não há mais reparo a fazer — irá registrar a ocorrência no arquivo de registro e sugerir ações alternativas. No exemplo mostrado na Figura 3-11, **Limpar** não é uma opção de ação disponível. Na maioria dos casos, você deve excluir esses arquivos e restaurá-los a partir de backups.

- **Excluir.** A Varredura de Correio Eletrônico excluirá imediatamente o arquivo do sistema. Como padrão, o programa incluirá o nome do arquivo infectado no registro, para que você possa restaurá-lo a partir de uma cópia de backup.

- **Mover.** A Varredura de Correio Eletrônico abre uma caixa de diálogo que pode ser usada para localizar a sua pasta de quarentena ou uma outra pasta adequada. Uma vez encontrada a pasta correta, clique em **OK** para transferir o arquivo para essa localização.

- **Informações.** A Varredura de Correio Eletrônico abre uma caixa de diálogo que exibe informações sobre o vírus ou o arquivo infectado. Esta opção não faz com que o programa realize qualquer ação contra o vírus detectado. Veja “Exibindo informações sobre o arquivo e o vírus” para obter mais detalhes.

Exibindo informações sobre o arquivo e o vírus

Clicar em **Informações** em qualquer uma das caixas de diálogo de ações contra vírus estabelecerá a conexão com a Biblioteca de informações sobre vírus online da Network Associates, contanto que você tenha uma conexão com a Internet e um software de navegador de web disponível em seu computador (Figura 3-13).
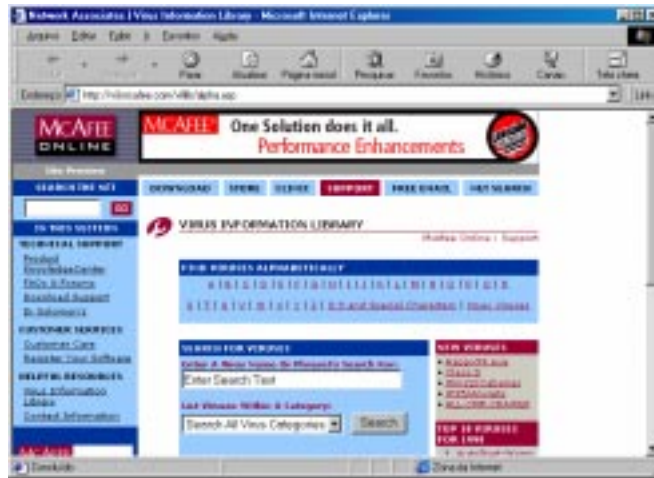
Figura 3-13. Biblioteca de informações sobre vírus online

A Biblioteca de informações sobre vírus contém documentos que proporcionam uma visão geral de cada vírus que o VirusScan pode detectar ou limpar. Essas informações incluem o modo como o vírus infecta e altera os arquivos, os tipos de cargas explosivas que desencadeiam, como reconhecer uma infecção e outros dados. A Biblioteca também fornece dicas sobre a maneira de impedir infecções por vírus e remover os vírus que o VirusScan não pode limpar nos arquivos infectados.

Se você escolher **Informações do arquivo** no menu **Arquivo**, na janela principal do VirusScan (veja Figura 3-10 na página 75) ou clicar com o botão direito em um arquivo na lista na janela principal do VirusScan ou na janela da Varredura de Correio Eletrônico (veja Figura 3-12 na página 78), em seguida selecionar **Informações do arquivo** no menu de atalho mostrado, o VirusScan abrirá uma caixa de diálogo Informação sobre o item infectado, onde aparece o nome do arquivo, seu tipo e tamanho em bytes e informação sobre as datas de criação e modificação, além da descrição de seus atributos (veja Figura 3-14 na página 80).

Figura 3-14. Página de propriedades Informações sobre arquivo infectado

Compreendendo os alarmes falsos

Uma alarme falso ocorre quando o VirusScan envia uma mensagem de alerta contra vírus ou cria uma entrada no arquivo de registro que identifica um vírus onde nenhum existe. É mais provável que você veja alarmes falsos se tiver mais de um software antivírus instalado no seu computador, porque alguns softwares antivírus armazenam as assinaturas de código usadas para detecção desprotegidas na memória.

A atitude mais segura a tomar quando você recebe um mensagem de alerta ou entrada de registro é tratá-la como uma ameaça real e realizar as etapas adequadas para remover o vírus de seu sistema. Se, contudo, acreditar que o VirusScan gerou um alarme falso — por exemplo, ele identificou um arquivo como infectado que você já usou sem problemas durante anos — verifique se não está incorrendo em uma dessas situações antes de entrar em contato com a Network Associates:

- **Você está executando mais de um programa antivírus.** Se esse for o caso, o VirusScan deve detectar assinaturas de códigos desprotegidas utilizadas por outro programa e relata-as como um vírus. Para evitar esse problema, configure o seu computador para que execute apenas um programa antivírus, em seguida feche o computador e desligue a energia. Aguarde alguns segundos antes de reiniciar o computador para que o sistema possa limpar as outras seqüências de caracteres de assinaturas de código do outro programa que estejam na memória.
- **Há um chip de BIOS com recursos antivírus.** Alguns chips de BIOS fornecem recursos antivírus que podem acionar alarmes falsos quando o VirusScan é executado. Consulte o guia do usuário do seu computador para saber como funcionam esses recursos antivírus e como desativá-los, se necessário.
- **Você tem um antigo PC da Hewlett-Packard ou da Zenith.** Alguns modelos antigos desses fabricantes modificam os setores de inicialização nos seus discos rígidos sempre que são inicializados. O VirusScan deve detectar essas alterações como vírus, quando não o são. Consulte o guia do usuário do seu computador para saber se é utilizado o código de inicialização automodificável. Para solucionar o problema, use a versão para linha de comando do VirusScan para adicionar informações sobre validação nos arquivos de inicialização. Esse método não salva as informações sobre o setor de inicialização ou o registro de inicialização mestre.
- **Você tem um software protegido contra cópia.** Dependendo do tipo de proteção contra cópia utilizado, o VirusScan deve detectar um vírus no setor de inicialização ou no registro de inicialização mestre em alguns disquetes ou em outros meios.

Se nenhuma dessas situações for aplicável, entre em contato com o suporte técnico da Network Associates ou envie uma mensagem de correio eletrônico para AVresearch@nai.com com uma explicação detalhada do problema ocorrido.

Usando o VShield 4

O que faz o VShield?

O VShield examina o sistema em segundo plano, enquanto você trabalha com os seus arquivos, para proteger o computador contra os vírus trazidos pelos disquetes, inserido através da rede, incorporados em anexos de arquivos de mensagens de correio eletrônico, ou carregados na memória. O programa é iniciado junto com o sistema e continua na memória até que o computador seja desligado. O VShield inclui também uma tecnologia que protege o sistema contra miniaplicativos Java e controles ActiveX hostis, e impede que o computador conecte-se a sites da Internet perigosos. Uma proteção por senha eficiente para as opções de configurações evita que outras pessoas façam alterações não autorizadas.

Por que usar o VShield?

O VShield contém recursos únicos que o tornam uma parte integral do pacote de segurança antivírus completo do VirusScan. Essas funcionalidades incluem:

- **"Varredura "ao acessar".** Esse recurso faz com que o VShield examine a ocorrência de vírus nos arquivos que são abertos, copiados, salvados ou modificados de qualquer forma, além de também nos que são lidos ou gravados em disquetes. Assim, o VShield pode detectar e impedir a propagação dos vírus logo que apareçam no sistema. Isto lhe oferece uma medida extra de proteção antivírus entre cada operação de varredura realizada.

- **Detecção e bloqueio de objetos destrutivos.** O VShield pode bloquear o acesso de objetos ActiveX e Java destrutivos ao seu sistema, antes que se tornem uma ameaça. O programa examina as centenas de objetos obtidos por download, logo que você conecta-se à Web ou a outros sites da Internet, além dos anexos de arquivos recebidos através do correio eletrônico. Compara esses itens a uma lista atualizada de objetos destrutivos que o programa mantém e bloqueia aqueles que podem causar problemas.

- **Filtragem de site da Internet.** O VShield contém uma lista de sites da Internet ou da Web perigosos que podem causar danos ao seu sistema, normalmente em forma de softwares destrutivos obtidos por download. Você pode adicionar qualquer outro site que desejar para que o software de navegação utilizado não se conecte a esse site, inserindo na lista o seu endereço de Protocolo Internet (IP) ou o nome de seu domínio.

- **Operação automática.** O VShield integra-se com uma ampla gama de softwares de navegadores e aplicativos de clientes de correio eletrônico com base na Messaging Application Programming Interface (MAPI) padrão da Microsoft. Isto permite que o VShield estabeleça uma conexão para examinar os seus anexos de correio eletrônico em busca de vírus, antes que eles atinjam o seu computador.

Quais navegadores e clientes de correio eletrônico o VShield aceita?

O VShield trabalha de forma integrada com muitos dos mais populares navegadores da Web e softwares de clientes de correio eletrônico disponíveis para a plataforma Windows. Para funcionar com o seu navegador, o VShield não necessita de configuração além da que você já definiu para conectar o seu computador à Internet. Contudo, o VShield deve ser configurado para funcionar corretamente com o software de cliente de correio eletrônico. Veja “Usando o assistente de configuração do VShield” na página 85 ou “Configurando as propriedades do VShield” na página 91 para saber como realizar a configuração necessária.

Os navegadores da Web testados e que funcionam corretamente com o VShield são:

- Netscape Navigator v3.x
- Netscape Navigator v4.0.x (não inclui a v4.0.6)
- Microsoft Internet Explorer v3.x
- Microsoft Internet Explorer v4.x

Os clientes de correio eletrônico testados e que funcionam corretamente com o módulo Varredura de Download do VShield são:

- Microsoft Outlook Express
- Qualcomm Eudora v3.x e v4.x
- Netscape Mail (incluído na maioria das versões do Netscape Navigator e Netscape Communicator)
- America Online mail v3.0 e v4.0

Para trabalhar com o módulo Varredura de Correio Eletrônico do VShield, você deve usar versões específicas do Lotus cc:Mail ou o seu software de cliente de correio eletrônico deve aceitar o padrão MAPI da Microsoft.
O clientes testados e que funcionam corretamente com o módulo Varredura de Correio Eletrônico são:

- Microsoft Exchange v4.0, v5.0 e v5.5
- Microsoft Outlook 97 e Outlook 98
- Lotus cc:Mail v6.x e v7.x (não compatível com MAPI)
- cc:Mail v8.0 e v8.01 (somente a versão compatível com MAPI)

Outros softwares de clientes compatíveis com MAPI poderão, muito provavelmente, funcionar de modo correto com o VShield, mas a Network Associates não certifica essa compatibilidade dos softwares de clientes que não estejam incluídos na lista acima.

Usando o assistente de configuração do VShield

Depois que o VirusScan é instalado e o computador reiniciado, o VShield é carregado imediatamente na memória e começa a trabalhar com um conjunto de opções padrão, que fornecem uma proteção contra vírus básica. A menos que você o desative ou a um de seus módulos — ou pare-o completamente — não é necessário se preocupar em iniciar o VShield ou planejar suas tarefas de varredura.

Contudo, para assegurar mais do que um nível mínimo de segurança, o VShield deve ser configurado para trabalhar com o software de cliente de correio eletrônico, a fim de examinar detidamente o seu tráfego de Internet em busca de vírus e softwares destrutivos. O assistente de configuração do VShield pode ajudar a definir muitas dessas opções imediatamente — em seguida, o programa pode ser configurado para funcionar melhor em seu ambiente, quando você estiver mais familiarizado com o VShield e com a suscetibilidade do seu sistema aos softwares destrutivos.

Para iniciar o assistente de configuração do VShield, execute uma das seguintes opções:

- Inicie o Programador de Tarefas do VirusScan, em seguida selecione o ícone do VShield na lista de tarefas. Depois clique em na barra de ferramentas do Programador de Tarefas. Para saber como iniciar e usar o Programador de Tarefas do VirusScan, veja “Iniciando o Programador de Tarefas do VirusScan” na página 184; ou
- Localize o ícone do VShield na barra de sistema do Windows, em seguida, pressione o botão direito do mouse. Aponte para **Propriedades** no menu de atalho mostrado, em seguida, escolha **Varredura do Sistema**. barra de tarefas

Qualquer um dos métodos abre a caixa de diálogo Propriedades do VShield (Figura 4-1).
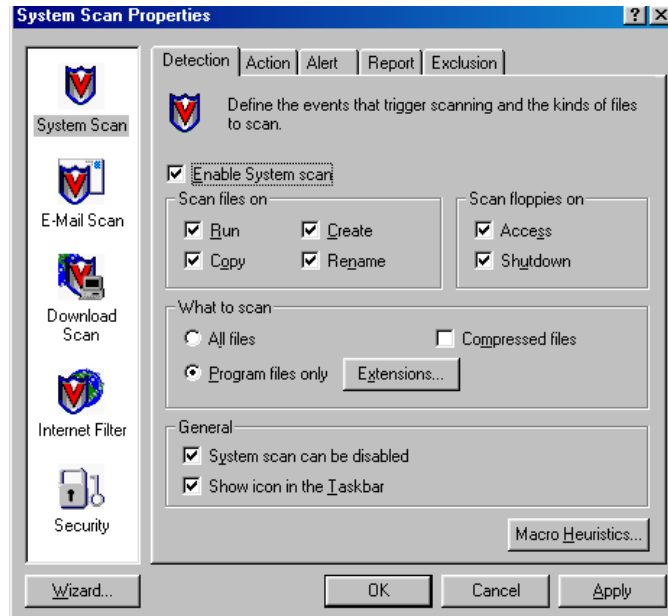
Figura 4-1. Caixa de diálogo Propriedades do VShield

Clique em **Assistente** no canto inferior esquerdo da caixa de diálogo para exibir o primeiro painel do assistente de configuração (Figura 4-2).

Figura 4-2. Assistente de Configuração do VShield - painel Bem-vindo

Clique em **Avançar>** para exibir o painel de configuração da Varredura do Sistema (Figura 4-3).

Figura 4-3. Assistente de Configuração do VShield - painel Varredura do Sistema

Neste painel, você pode instruir o VShield a procurar vírus nos arquivos suscetíveis a infecção sempre que forem abertos, executados, copiados, salvados ou modificados de qualquer forma. Os arquivos suscetíveis incluem vários tipos de arquivos executáveis e de documentos com macros incorporadas, como os arquivos do Microsoft Office. O VShield examinará também os arquivos armazenados em disquetes sempre que forem lidos ou recebam gravação, ou quando o computador for desligado.

Se encontrar um vírus, o VShield emitirá um alerta sonoro e lhe solicitará uma ação. O programa também irá registrar suas ações e resumir as configurações atuais em um arquivo de registro que você pode rever posteriormente.

Para ativar essas funções, selecione **Sim**, em seguida, clique em **Avançar>**. Caso contrário, selecione **Não** e clique em **Avançar>** para continuar.

Aparece o painel do assistente da Varredura de Correio Eletrônico (Figura 4-4 na página 88).

Figura 4-4. Assistente de Configuração do VShield - painel Varredura de Correio Eletrônico

Se você não usar correio eletrônico ou não conectar-se à Internet, marque a caixa de verificação **Não uso correio eletrônico**, em seguida, clique em **Avançar>** para continuar. Caso contrário, marque a caixa de verificação que corresponda ao tipo de cliente de correio eletrônico utilizado. Estas são as opções:

- **Ativar correio eletrônico corporativo.** Marque esta caixa de verificação se você usar um sistema de correio eletrônico patenteado, no trabalho ou em um ambiente de rede. A maioria dos sistemas de correio eletrônico utiliza um servidor de rede central para receber e distribuir correio, que usuários individuais enviam uns para os outros a partir de aplicativos de clientes. Esses sistemas podem enviar e receber correio de fora da rede ou na Internet, mas, normalmente, o fazem através de um aplicativo do tipo "gateway" executado no servidor.

  O VShield aceita sistemas de correio eletrônico corporativos que se enquadrem em duas categorias gerais:

  – **Cliente de correio eletrônico compatível com MAPI**. Selecione este botão se você usar um cliente de correio eletrônico que seja compatível com o MAPI padrão. Os exemplos desses clientes incluem Microsoft Exchange, Microsoft Outlook e a versão 8.0 ou posterior do Lotus cc:Mail.

  – **Lotus cc:Mail.** Selecione este botão se você estiver usando o cc:Mail versões 6.x ou 7.x, que usa um protocolo da Lotus patenteado para enviar e receber correio.

- **Clientes de correio eletrônico da Internet.** Marque esta caixa de verificação se você estiver usando um cliente de correio eletrônico Post Office Protocol (POP-3) ou Simple Mail Transfer Protocol (SMTP), que envia e recebe correio da Internet padrão diretamente ou através de uma conexão de discagem. Se o correio for enviado e recebido em casa através do Netscape Mail, America Online ou clientes populares como o Eudora da Qualcomm ou o Outlook da Microsoft, certifique-se de ter selecionado essa opção

Após especificar o sistema de correio eletrônico utilizado, clique em **Avançar>** para continuar.

NOTA: Se forem utilizados ambos os tipos de sistemas de correio, marque as duas caixas de verificação. Contudo, observe que o VShield aceita apenas um tipo de sistema de correio eletrônico *corporativo* de cada vez. Se for necessário verificar qual sistema de correio é utilizado no seu escritório, pergunte ao seu administrador da rede.

Confirme também se você sabe qual é a diferença entre o Microsoft Outlook e o Microsoft Outlook Express. Embora os nomes dos programas sejam semelhantes, o Outlook 97 e o Outlook 98 são sistemas de correio eletrônico corporativos compatíveis com MAPI, porém o Outlook Express envia e recebe correio eletrônico através dos protocolos POP-3 e SMTP. Para saber mais sobre esses programas, consulte a documentação da Microsoft.

O próximo painel do assistente configura as opções para o módulo Varredura de Download (Figura 4-5).

Figura 4-5. Assistente de Configuração do VShield - painel Varredura de Download

Para que o VShield procure vírus em cada arquivo obtido por download na Internet, marque a caixa de verificação **Procurar vírus nos arquivos obtidos por download**, em seguida, clique em **Avançar>** para continuar. O VShield irá procurar vírus nesses arquivos mais suscetíveis a infecção e examinará os arquivos compactados à medida que forem recebidos.

Caso contrário, marque a caixa de verificação **Não ativar varredura de download**, em seguida, clique em **Avançar>** para continuar.

O próximo painel do assistente configura as opções para o módulo Filtro de Internet do VShield (veja Figura 4-6).

Figura 4-6. Assistente de Configuração do Vshield – painel Filtro de Internet

Selecione **Sim, ativar proteção contra miniaplicativo hostil e impedir o acesso a sites da web perigosos**, em seguida clique em **Avançar>** para que o VShield bloqueie os miniaplicativos Java e controles ActiveX que podem causar danos ao sistema. Essa opção impedirá o seu navegador da Web de conectar-se a sites de Internet ou da Web potencialmente perigosos. O VShield mantém atualizada uma lista de objetos e sites destrutivos que é utilizada para verificar os sites visitados e os objetos encontrados. Se for encontrada uma coincidência, o VShield poderá bloquear o site automaticamente ou oferecer-lhe a opção de negar ou conceder acesso.

Para desativar essa função, selecione **Não ativar proteção contra miniaplicativo hostil e impedir o acesso a sites da web perigosos**, em seguida, clique em **Avançar>** para continuar.

O painel final do assistente resume as opções escolhidas (Figura 4-7).
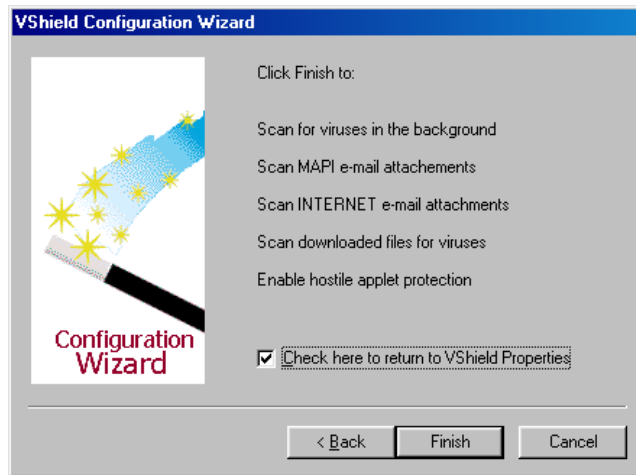
Figura 4-7. Assistente de Configuração do VShield - painel de resumo

Se a lista de resumos refletir precisamente as suas opções, clique em **Concluir** para salvar as suas alterações e retornar à caixa de diálogo Propriedades do VShield. Caso contrário, clique em **<Voltar** para alterar as opções escolhidas, ou **Cancelar** para retornar à caixa de diálogo Propriedades do VShield sem salvar as alterações.

Configurando as propriedades do VShield

Para assegurar o melhor desempenho no seu computador ou no ambiente de rede, é necessário informar ao VShield o que é preciso examinar, o que fazer no caso de encontrar um vírus ou um software destrutivo e como avisá-lo dessas ocorrências. Você pode usar o assistente de configuração para ativar a maioria das opções de proteção do VShield, mas se quiser ter controle total sobre o desempenho do programa e poder adaptá-lo à suas necessidades, escolha as opções na caixa de diálogo Propriedades do VShield.

A caixa de diálogo Propriedades do VShield consiste de uma série de páginas de propriedades que controlam as configurações de cada módulo do programa. Para escolher as suas opções, clique no ícone do módulo de programa adequado, em seguida, clique em cada guia de uma vez, na caixa de diálogo Propriedades do VShield.

Para abrir a caixa de diálogo Propriedades do VShield, escolha uma das opções:

- Inicie o Programador de Tarefas do VirusScan, em seguida selecione o ícone do VShield na lista de tarefas. Em seguida, clique em na barra de ferramentas do Programador de Tarefas. Para saber como iniciar e usar o Programador de Tarefas do VirusScan, veja "Iniciando o Programador de Tarefas do VirusScan" na página 184; ou

- Localize o ícone do VShield na barra de sistema do Windows, em seguida, pressione o botão direito do mouse. Aponte para **Propriedades** no menu de atalho mostrado, em seguida, escolha **Varredura do Sistema**. barra de tarefas

Qualquer um dos métodos abre a caixa de diálogo Propriedades do VShield (Figura 4-8).
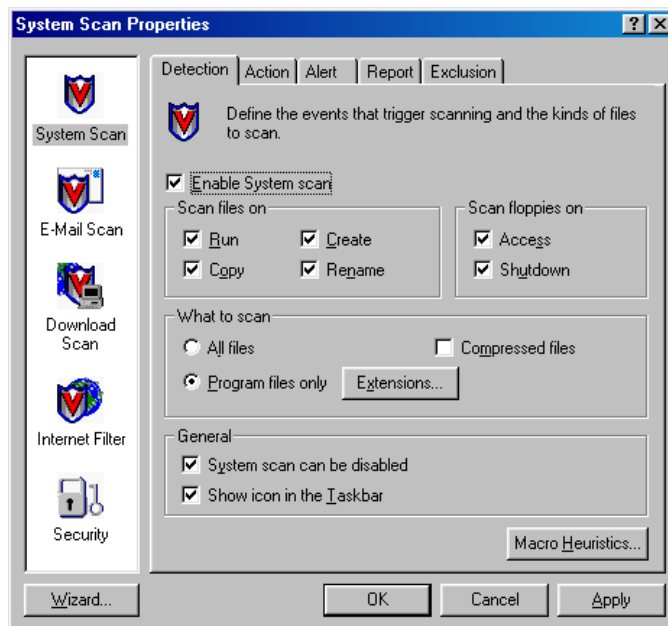
Figura 4-8. Caixa de diálogo Propriedades da Varredura do Sistema - página Detecção

Configurando o módulo Varredura do Sistema

O módulo Varredura do Sistema do VShield procura vírus no seu sistema sempre que você abrir, executar, salvar ou modificar arquivos no disco rígido, e quando um disquete for lido ou gravado. Para escolher as suas opções, clique no ícone da Varredura do Sistema, no lado esquerdo da caixa de diálogo Propriedades do VShield, a fim de exibir as páginas de propriedades para esse módulo. As seções seguintes descrevem as opções.

Escolhendo opções de Detecção

O VShield supõe inicialmente que é necessário procurar vírus sempre que você trabalha com um arquivo suscetível a infecção, que esteja no disco rígido ou em um disquete (veja Figura 4-8 na página 92). Embora essas opções padrão ajustem o desempenho da varredura à segurança, o seu ambiente pode necessitar de configurações diferentes.

Para modificá-las, verifique se a caixa de verificação Ativar a Varredura do Sistema está marcada, em seguida, realize as etapas abaixo:

1. Informe quando e onde o VShield deve procurar vírus. O programa pode Examinar arquivos enquanto são utilizados.

   - **Examinar arquivos enquanto são utilizados.** Sempre que você abre, copia, salva, renomeia ou usa de alguma forma os arquivos no disco rígido, o código do vírus pode ser executado e espalhar infecções para outros arquivos. Para evitar isso, selecione qualquer combinação das caixas de verificação **Executar**, **Copiar**, **Criar** e **Renomear** — a seleção de todas as opções garante a melhor segurança. O VShield aumentará ligeiramente o tempo de cada operação ao examinar cada arquivo.

   - **Examinar arquivos em disquetes.** Os vírus de setor de inicialização podem ocultar-se nos blocos de inicialização de qualquer disquete formatado, em seguida são carregados na memória assim que o computador ler na unidade de disco. Marque a caixa de verificação **Acessar** para que o VShield examine os disquetes sempre que o computador os ler. Marque a caixa de seleção **Desligar** para que o VShield examine os disquetes deixados na unidade de disco quando o computador for desligado. Esse procedimento assegura que nenhum vírus poderá ser carregado quando o computador ler a unidade de disco durante a inicialização.

2. Especifique os tipos de arquivo que o VShield examinará. Você pode

- **Examinar arquivos compactados.** Marque a caixa de seleção **Arquivos compactados** para que a Varredura do Sistema procure vírus em arquivos compactados com LZEXE e PKLite. Embora esse procedimento lhe ofereça uma proteção melhor, esse exame pode tornar mais longa uma operação de varredura.

- **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Contudo, você pode reduzir seguramente a abrangência das operações de varredura a esses arquivos mais suscetíveis a infecções por vírus, a fim de acelerá-las. Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou determinar as extensões de nomes de arquivos que o VShield examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (Figura 4-9).
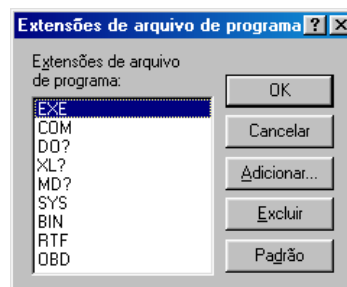
Figura 4-9. Caixa de diálogo Extensões de arquivo de programa

Como padrão, o VShield procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .MD?, .SYS, .BIN, .RTF e .OBD. Os arquivos com as extensões.DO?, .XL?, .RTF, .MD? e .OBD pertencem ao Microsoft Office, sendo que todos podem ser infectados por vírus de macro. O caractere ? é um curinga que possibilita ao VShield examinar arquivos de modelos e de documentos.

❒ **NOTA:** A lista de extensões de programa padrão do Vshield é diferente da lista do VirusScan, porque a varredura dos arquivos .DLL e .VXD — arquivos comuns usados constantemente pelo Windows — iria diminuir expressivamente o desempenho do sistema. Para que o VShield examine esses tipos de arquivos, adicione suas extensões na caixa de diálogo. Como alternativa, considere a execução das operações de varredura do VirusScan, se você precisar examinar esses tipos de arquivos regularmente.

– Para adicioná-las à lista, clique em **Adicionar**, em seguida, digite as extensões que o VShield deverá examinar na caixa de diálogo mostrada.

– Para remover uma extensão da lista, selecione-a, em seguida, clique em **Remover**.

– Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

- **Examinar todos os arquivos.** Para que o VShield examine os arquivos do sistema utilizados de qualquer forma, com qualquer extensão, selecione o botão **Todos os arquivos**. Isto reduzirá a velocidade do sistema consideravelmente, mas irá assegurar que estará sem vírus.

3. Escolha quais tipos de varredura heurística você deseja ativar. Clique em **Heurística** para abrir a caixa de diálogo Configurações da Varredura Heurística (Figura 4-10).
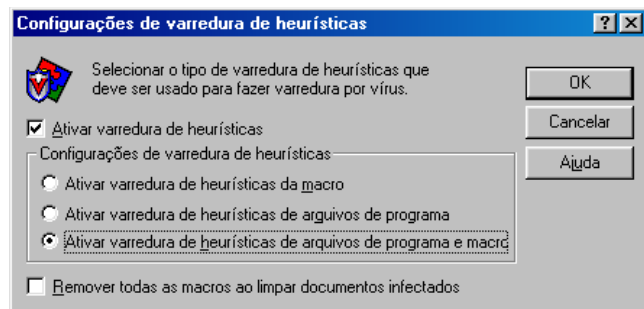
Figura 4-10. Caixa de diálogo Configurações da varredura heurística

A tecnologia da varredura heurística possibilita ao VShield reconhecer novos vírus com base na sua semelhança com vírus similares que o programa já conhece. Para fazê-lo, o VShield procura determinadas características “semelhantes a vírus” nos arquivos que você pediu para serem examinados. A presença de um número suficiente dessas características em um arquivo leva o VShield a identificar o arquivo como potencialmente infectado com um vírus novo ou que não foi identificado anteriormente.

Como o VShield procura simultaneamente as características de arquivo que excluam a possibilidade de infecção por vírus, raramente será dada uma informação falsa sobre uma infecção por vírus. Entretanto, a menos que você saiba que esse arquivo *não* contém um vírus, deverá tratar as infecções "prováveis" com o mesmo cuidado que as confirmadas.

Para ativar a varredura heurística, siga estas etapas

a. Marque a caixa de seleção **Ativar a varredura heurística**. As demais opções na caixa de diálogo são ativadas.

b. Selecione os tipos de varredura heurística que devem ser utilizadas pelo VShield. Estas são as opções:

   - **Ativar a varredura heurística de macro**. Escolha esta opção para que o VShield identifique todos os arquivos do Microsoft Word, Microsoft Excel e outros do Microsoft Office que tenham macros incorporadas, em seguida compare o código da macro com o banco de dados de assinaturas de vírus. O VShield identificará a correspondências exatas com o nome do vírus; as assinaturas de código semelhantes a de vírus existentes fazem com que o programa o informe que encontrou um provável vírus de macro.

   - **Ativar a varredura heurística de arquivos de programa.** Escolha esta opção para que o VShield localize novos vírus em arquivos de programa examinando as suas características e comparando-as a uma lista de especificações de vírus conhecidos. O programa identificará os arquivos com um número suficiente dessas características como vírus prováveis.

   - **Ativar a varredura heurística de arquivos de programa e macros.** Escolha esta opção para que o VShield use ambos os tipos de varredura heurística. A Network Associates recomenda que você use essa opção para obter uma proteção completa antivírus.

c. Determinar como deseja tratar os arquivos de macros infectados. Selecione **Remover todas as macros ao limpar documentos infectados** para eliminar todos os códigos infectantes do documento e deixar apenas os dados. Para tentar eliminar apenas os códigos de vírus das macros de documentos, não marque essa caixa de seleção.

> **ATENÇÃO:** Use esse recurso com cuidado: a remoção de todas as macros de um documento pode causar a perda de dados ou danificá-lo, tornando o documento inútil.

d. Clique em **OK** para salvar as suas configurações e retornar à caixa de diálogo Propriedades do VShield.

4. Escolher as opções de gerenciamento do VShield. Estas opções permitem controlar a sua interação com o VShield. Você pode

   - **Desative o módulo Varredura do Sistema quando quiser.** Marque a caixa de verificação **Desativar a Varredura do Sistema** para que a opção desative esse módulo. Observe que a Network Associates recomenda que a Varredura do Sistema deve ser mantida ativada para assegurar máxima proteção. Caso esta caixa seja desmarcada, o comando de desativação do menu de atalho do VShield e o botão de desativação na caixa de diálogo Status do VShield Status serão removidos.

     > **DICA:** Para assegurar que nenhuma outra pessoa que use o computador possa desativar o VShield, ou para promover a política de segurança antivírus entre os usuários do VirusScan em sua rede, desmarque essa caixa de verificação, em seguida, proteja as configurações com uma senha. Isto fará com que outros usuários não possam desativar o VShield do Programador de Tarefas do VirusScan, ou na caixa de diálogo Propriedades do VShield. Veja “Configurando o módulo Segurança” na página 143 para obter mais detalhes.

   - **Exibir o ícone do VShield na barra de sistema do Windows.** Marque a caixa de verificação **Mostrar ícone na barra de tarefas** para que o VShield exiba o seu ícone na área de trabalho do sistema. Dois cliques no ícone abrem a caixa de diálogo Status do VShield. Um clique com o botão direito no ícone exibe um menu de atalho. Veja “Usando o menu de atalho do VShield” na página 147 e “Controlando informações de status do VShield” na página 151 para obter mais detalhes.

5. Clique na guia Ação para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura do Sistema, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Ação

Quando o VShield detecta um vírus, poderá lhe perguntar o que deve fazer com o arquivo infectado ou atuar automaticamente utilizando uma ação predeterminada. Use a página de propriedades Ação para especificar quais opções de ação o VShield deve lhe propor ao encontrar um vírus ou quais ações o programa deve realizar automaticamente.

Siga estas etapas:

1. Clique na guia Ação no módulo Varredura do Sistema para exibir a página de propriedades correta (Figura 4-11).

Figura 4-11. Caixa de diálogo Propriedades da Varredura do Sistema – página Ação

2. Escolha uma ação na lista **Quando um vírus for encontrado**. A área imediatamente abaixo da lista será alterada para mostrar as opções adicionais para cada uma delas.

Estas são as opções:

- **Solicitar ação ao usuário.** Escolha esta opção se você quiser que o VShield o consulte sobre o que fazer quando encontrar um vírus — o programa exibirá uma mensagem de alerta e proporá opções de ação possíveis. Selecione as opções de ação que você deseja ver na mensagem de alerta:
  - **Limpar arquivo.** Esta opção informa ao VShield para tentar remover o código de vírus do arquivo infectado.
  - **Excluir arquivo.** Esta opção informa ao VShield para excluir o arquivo infectado imediatamente.
  - **Excluir o item da varredura.** Esta opção informa ao VShield para não examinar o arquivo a partir de agora.
  - **Continuar o acesso.** Esta opção informa ao VShield para continuar a trabalhar com o arquivo e não realizar nenhuma outra ação. Se as opções de relatório estiverem ativadas, o VShield incluirá a ocorrência no arquivo de registro. Esta opção também faz com que o VShield exiba um alerta de tela inteira em vez de uma caixa de diálogo quando encontrar um vírus. Veja “Reagindo quando o VShield detecta um software destrutivo” na página 69 para obter mais detalhes.
  - **Interromper o acesso.** Esta opção instrui o VShield a negar acesso ao arquivo, mas não executará nenhuma outra ação. A negação de acesso ao arquivo impede que você o abra, salve ou renomeie. Para continuar, clique em **OK**. Se você tiver ativado o recurso de relatório, o VShield registrará o incidente.
- **Mover arquivos infectados automaticamente**. Escolha esta opção para que o VShield mova os arquivos infectados para um diretório de quarentena logo após encontrá-los. Como padrão, o VShield move esses arquivos para uma pasta chamada INFECTADO, criada no nível raiz da unidade na qual o vírus foi encontrado. Por exemplo, se o VShield encontrar um arquivo infectado em T:\MEUS DOCUMENTOS e for especificada a pasta INFECTADO como o diretório de quarentena, o VShield copiará o arquivo para T:\INFECTADO.

  Você pode digitar um nome e um caminho diferentes na caixa de texto ou clicar em **Procurar** para localizar uma pasta adequada no disco rígido.

- **Limpar arquivos infectados automaticamente.** Escolha esta opção para informar ao VShield para remover o código do vírus do arquivo infectado assim que for encontrado. Se o VShield não puder remover o vírus, você receberá um aviso através de uma notificação na área de mensagem, e se os recursos de relatório estiverem ativados, a ocorrência será incluída no arquivo de registro. Veja o "Escolhendo opções de Relatório" na página 102 para obter mais detalhes.

- **Excluir arquivos infectados automaticamente.** Escolha esta opção para que o VShield exclua imediatamente os arquivos infectados encontrados. Certifique-se de ter ativado o recurso de relatório para que você tenha um registro de quais arquivos o VShield excluiu. Será necessário restaurar os anexos excluídos a partir de cópias de backup.

- **Negar acesso a arquivos infectados e continuar.** Escolha esta opção para informar ao VShield para marcar o arquivo como "fora do limite" e continuar as operações de varredura normal. Selecione esta opção apenas se você planeja afastar-se do computador durante longos períodos. Se o recurso de relatório também estiver ativado (veja "Escolhendo opções de Relatório" na página 102 para obter mais detalhes), o programa registrará os nomes dos vírus encontrados e os nomes dos arquivos infectados para que você possa eliminá-los na próxima oportunidade.

3. Clique na guia Alerta para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura do Sistema, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Alerta

Após configurá-lo com as opções de ação desejadas, o VShield irá procurar vírus no sistema e remover automaticamente os encontrados, sem que sejam necessárias outras interferências. Se, contudo, for possível configurar o VShield para avisar-lhe imediatamente após encontrar um vírus, a fim de que você possa realizar a ação necessária, é possível configurá-lo para enviar uma mensagem de alerta para você ou outras pessoas de várias maneiras. Use a página de propriedades Alerta para escolher quais métodos de Alerta serão utilizados.

Siga estas etapas:

1. Clique na guia Alerta do módulo Varredura do Sistema para exibir a página de propriedades correta (Figura 4-12).
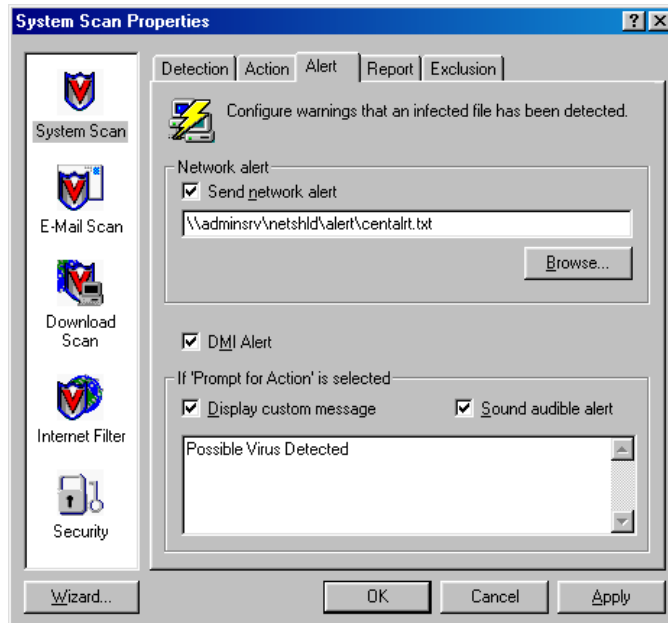
Figura 4-12. Caixa de diálogo Propriedades da Varredura do Sistema – página Alerta

2. Para informar ao VShield que envie uma mensagem de alerta a um servidor que esteja executando o NetShield , uma solução antivírus com base em servidor da Network Associates, marque a caixa de verificação **Enviar alerta de rede**, em seguida, digite o caminho para a pasta de alertas do NetShield na sua rede ou clique em **Procurar** para localizar a pasta correta.

NOTA: A pasta escolhida deve conter o CENTALRT.TXT, o arquivo Alerta Centralizado do NetShield. Esse programa coleta as mensagens de alerta do VShield e de outros softwares da Network Associates, em seguida, passa-os para os administradores de rede para que realizem as ações necessárias. Para saber mais sobre o Alerta Centralizado, veja o *Guia do Usuário* do NetShield.

---

3. Para que o VShield envie mensagens de alerta sobre vírus através da interface de componente DMI para a área de trabalho e para os aplicativos de gerenciamento que estejam sendo executados na rede, marque a caixa de verificação **Alerta DMI**.

> **NOTA:** A Desktop Management Interface é um padrão para comunicação de solicitações de gerenciamento e informações sobre alertas entre componentes de hardware e software armazenados em ou conectados a computadores de mesa, e os aplicativos utilizados para gerenciá-los. Para saber mais sobre a utilização desse método de alerta, consulte o administrador da rede.

4. Se você escolher **Solicitar ação ao usuário** como a sua opção na página Ação (veja “Escolhendo opções de Ação” na página 98 para obter mais detalhes), também poderá informar ao VShield que emita um sinal sonoro e exiba uma mensagem personalizada ao encontrar um vírus. Para fazer isso, marque a caixa de verificação **Exibir mensagem personalizada** em seguida, digite a mensagem que aparecerá na caixa de texto mostrada — pode ser digitada uma mensagem com 225 caracteres, no máximo. Depois, marque a caixa de verificação **Soar alerta audível**.

5. Clique na guia Relatório para escolher as opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura do Sistema, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

> **NOTA:** O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Relatório

O módulo Varredura do Sistema do VShield contém uma lista com as configurações atuais e resume todas as ações efetuadas, durante as operações de varredura, em um arquivo de registro chamado VSHLOG.TXT. O VShield poderá gravar o registro nesse arquivo ou usar um arquivo de texto criado com qualquer editor de texto. Esse arquivo de registro pode ser aberto e impresso para revisão posterior em qualquer editor de texto.

O arquivo VSHLOG.TXT pode servir como uma importante ferramenta de gerenciamento para controlar a atividade de vírus no sistema e anotar quais configurações foram usadas para detectar e atuar contra as infecções encontradas pelo VShield. Você também pode utilizar os relatórios de ocorrências registrados no arquivo para determinar quais arquivos é necessário substituir a partir de cópias de backup, examinar na pasta de quarentena ou excluir do seu computador. Use a página de propriedades Relatório para determinar quais informações o VShield incluirá no arquivo de registro.

Para configurar o VShield a fim de registrar suas ações em um arquivo de registro, siga estas etapas:

1. Clique na guia Relatório do módulo Varredura do Sistema para exibir a página de propriedades correta (Figura 4-13).

Figura 4-13. Caixa de diálogo Propriedades da Varredura do Sistema – página Relatório

2. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, o VShield grava as informações de registro no arquivo VSHLOG.TXT no diretório de programas do VirusScan. Você pode digitar um nome e um caminho diferentes na caixa de texto mostrada, ou clicar em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

3. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o VShield limita o tamanho de arquivo em 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, o VShield apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

4. Marque as caixas de verificação correspondentes às informações que o VShield deverá incluir no arquivo de registro. Você pode optar por gravar estas informações:

   - **Detecção de vírus.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados, encontrados durante esta sessão de varredura.

   - **Limpeza de vírus.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados dos quais removeu os vírus.

   - **Eliminação do arquivo infectado.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados que ele excluiu do sistema.

   - **Movimentação do arquivo infectado.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados que ele moveu para o diretório de quarentena.

   - **Configurações da sessão.** Marque esta caixa de verificação para que o VShield faça uma lista das opções escolhidas na caixa de diálogo Propriedades da Varredura do Sistema para cada sessão de varredura.

- **Resumo da sessão.** Marque esta caixa de verificação para que o VShield faça um resumo das suas ações durante cada sessão de varredura. As informações do resumo incluem o número de arquivos examinados pelo VShield, o número e o tipo de vírus detectados, o número de arquivos movidos ou excluídos, e outras informações.

- **Data e hora.** Marque esta caixa de verificação para que o VShield anexe a data e a hora a cada entrada do registro incluída.

- **Nome do usuário.** Marque esta caixa de verificação para que o VShield anexe o nome do usuário conectado ao seu computador no momento que incluir cada entrada de registro.

5. Clique na guia Exclusão a fim de escolher as opções do VShield opcionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura do Sistema, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Exclusão

Muitos dos arquivos armazenados no seu computador não são vulneráveis a infecções por vírus. O exame desse arquivos pelo VShield pode ocupar um longo tempo e produzir poucos resultados. Você pode acelerar as operações de varredura informando ao VShield para examinar os tipos de arquivos suscetíveis a infecções (veja “Escolhendo opções de Detecção” na página 93 para obter mais detalhes) ou instrui-lo para ignorar arquivos ou pastas inteiras que não serão infectados.

Após usar o VirusScan para examinar completamente o seu sistema, você pode informar ao VShield para ignorar os arquivos e pastas que não são modificados ou que não sejam vulneráveis, normalmente, a infecção por vírus. Para que o VShield não examine determinados arquivos e pastas, siga estas etapas:

1. Clique na guia Exclusão do módulo Varredura do Sistema para exibir a página de propriedades correta (Figura 4-14 na página 106).
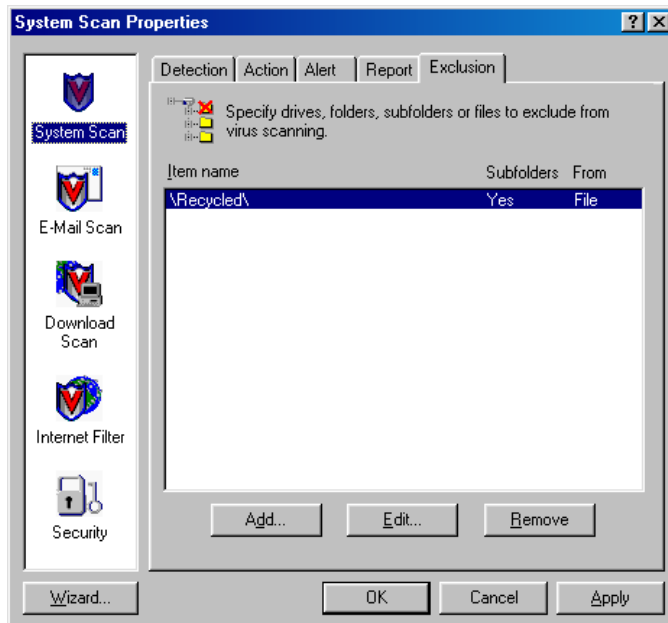
Figura 4-14. Caixa de diálogo Propriedades da Varredura do Sistema – página Exclusão

A página Exclusão criará inicialmente uma lista com apenas o conteúdo da Lixeira. O VShield elimina a Lixeira de reciclagem das operações de varredura porque o Windows não executará os arquivos nela armazenados.

2. Especifique os itens a serem excluídos. Você pode

   - **Adicionar arquivos, pastas e volumes à lista de exclusão.** Clique em **Adicionar** para abrir a caixa de diálogo Adicionar item para exclusão (Figura 4-15).
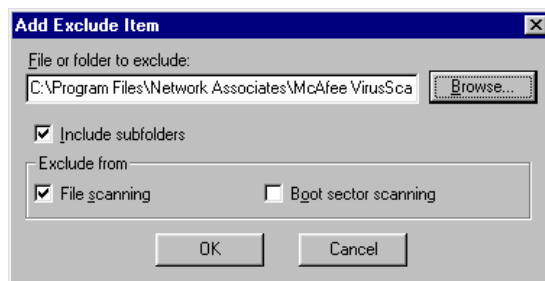
Figura 4-15. Caixa de diálogo Adicionar item para exclusão

a. Caixa de diálogo Adicionar item de exclusão de varredura Digite o volume, o caminho para o arquivo ou para a pasta que você deseja excluir da varredura, ou clique em **Procurar** para localizar um arquivo ou pasta no seu computador.

NOTA: Se você tiver escolhido mover os arquivos infectados para um pasta de quarentena automaticamente, o VShield não examinará essa pasta.

---

b. Marque a caixa de verificação **Incluir subpastas** para excluir todas as subpastas contidas na pasta especificada.

c. Marque a caixa de seleção **Varredura de arquivo** para que o VShield não procure vírus infectantes nos arquivos ou nas pastas excluídas.

d. Marque a caixa de verificação **Varredura de setor de inicialização** para informar ao VShield que não procure vírus de setor de inicialização nos arquivos ou pastas excluídas. Use essa opção para excluir arquivos de sistema, como COMMAND.COM, das operações de varredura.

ATENÇÃO: A Network Associates recomenda que você *não* exclua os seus arquivos de sistema da varredura em busca de vírus.

---

e. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo.

f. Repita as etapas A a D até incluir na lista todos os arquivos e pastas que não devem ser examinados.

- **Alterar a lista de exclusão.** Para alterar as configurações de um item de exclusão, selecione-o na lista Exclusões, em seguida, clique em **Editar** para abrir a caixa de diálogo Editar item de exclusão de varredura. Faça as alterações necessárias, em seguida, clique em **OK** para fechar a caixa de diálogo.

- **Remover um item da lista.** Para remover um item de exclusão, selecione-o na lista, em seguida, clique em **Remover**. O VShield examinará esse arquivo ou pasta durante a próxima operação de varredura.

3. Clique em uma guia diferente para alterar qualquer uma das configurações da Varredura do Sistema, ou clique em um dos ícones na lateral da caixa de diálogo Propriedades da Varredura do Sistema para escolher opções para outro módulo.

   Para salvar as alterações no módulo Varredura do Sistema sem fechar a caixa de diálogo, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

   NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Configurando o módulo Varredura de Correio Eletrônico

O módulo Varredura de Correio Eletrônico do Shield procura vírus em arquivos anexados a mensagens de correio eletrônico recebidas através de sistema de correio eletrônico corporativo, como Microsoft Exchange, Microsoft Outlook ou Lotus cc:Mail, ou através de programas de clientes POP-3 ou SMTP de correio eletrônico, como Eudora, Netscape Mail ou Microsoft Outlook Express. O VShield concentra-se nos anexos de arquivos incluídos nas suas mensagens de correio eletrônico, pois as mensagens em si, com raras excessões, não são normalmente vulneráveis a infecções. Como o programa pode examinar correio eletrônico logo que aparece no seu servidor de correio eletrônico ou na sua área de trabalho, poderá interceptar os vírus antes que possam espalhar-se.

Para escolher as suas opções, clique no ícone da Varredura de Correio Eletrônico no lado esquerdo da caixa de diálogo Propriedades do VShield a fim de exibir as páginas de propriedades para esse módulo. As seções seguintes descrevem as opções.

Escolhendo opções de Detecção

O VShield não ativa o módulo Varredura de Correio Eletrônico como padrão, a menos que você já tenha usado o seu assistente de configuração para escolher as suas opções, porque o programa precisa saber qual o sistema de correio eletrônico utilizado.

Para ativar e configurar a Varredura de Correio Eletrônico, siga estas etapas:

1. Marque a caixa de verificação **Ativar a varredura de anexos de correio eletrônico**.

   As opções restantes na página de propriedades são ativadas (Figura 4-16).
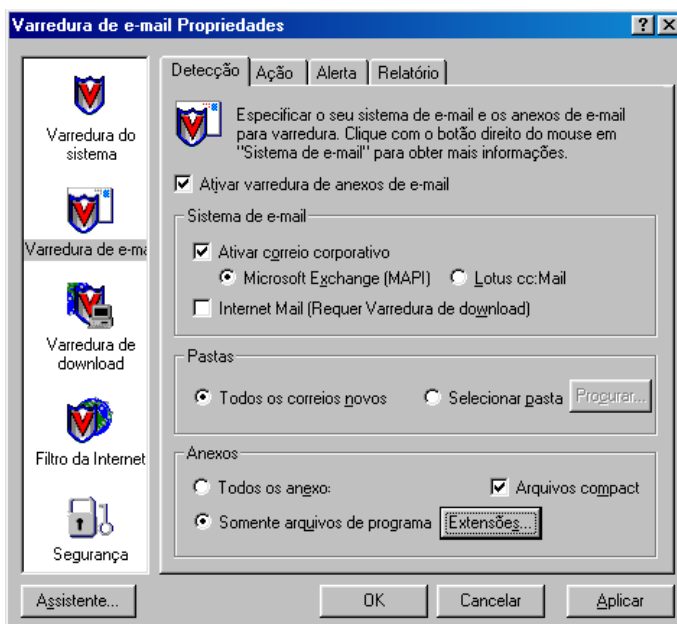
Figura 4-16. Caixa de diálogo Propriedades da Varredura de Correio Eletrônico - página Detecção

2. Selecione o tipo de sistema de correio eletrônico utilizado. Estas são as opções:

   - **Ativar correio eletrônico corporativo.** Marque essa caixa de seleção para que o VShield examine os anexos de correio recebidos através de um sistema de correio na rede de seu escritório. Normalmente, esses sistemas usam um protocolo de correio patenteado e têm um servidor de correio central para o qual você envia o correio a ser expedido. Com freqüência, esses sistemas enviam e recebem correio de Internet, mas geralmente o fazem através de um aplicativo de gateway. O módulo Varredura de Correio Eletrônico dá suporte a dois tipos de sistemas de correio eletrônico corporativos:

     – **Microsoft Exchange (MAPI).** Selecione este botão se você utilizar um sistema de correio eletrônico que envia e recebe mensagens através da Messaging Application Programming Interface da Microsoft, um protocolo de correio do Windows. Os exemplos incluem Microsoft Exchange, Microsoft Outlook 97 e Outlook 98, Lotus cc:Mail 8.0 e cc:Mail 8.01.

     – **Lotus cc:Mail.** Selecione este botão se você utilizar o cc:Mail 6.x ou 7.x. Esses sistemas usam um protocolo da Lotus patenteado para enviar e receber correio eletrônico. O cc:Mail versão 8.0 ou posterior também pode ser instalado de forma a usar o mesmo protocolo que as versões anteriores do cc:Mail. Para verificar qual o sistema usado, consulte o administrador da rede.

NOTA: Para ver a opção **Lotus cc:Mail**, você deve usar a opção Instalação Personalizada do VirusScan para instalar o componente de varredura cc:Mail do VirusScan. Veja o Capítulo 2, página 42 para obter mais detalhes. Você pode selecionar apenas um sistema de correio eletrônico *corporativo* de cada vez, mas poderá fazer com que o VShield examine todos os anexos recebidos pelos sistemas de correio eletrônico corporativo e da Internet, caso utilize ambos.

- **Correio da Internet (Requer a Varredura de Download).** Marque essa caixa de seleção para que o VShield examine o correio da Internet recebido e enviado através do Post Office Protocol (POP-3) ou do Simple Mail Transfer Protocol (SMTP). Escolha esta opção se você trabalhar em casa ou comunicar-se através de um provedor de serviços de discagem da Internet, usando um software como o Eudora Pro da Qualcomm, Outlook Express da Microsoft ou Netscape Mail.

  IMPORTANTE: Como você recebe o correio da Internet e outros arquivos obtidos por download através do mesmo "pipe", o VShield usa as opções de detecção, ação, alerta e relatório definidas no módulo Varredura de Download para determinar como atuar em relação à entrada de correio da Internet. Contudo, para examinar os anexos do correio da Internet, deve ser ativado também o módulo Varredura de Download e utilizadas as páginas de propriedades para escolher as configurações desejadas.

3. Informe ao VShield quais origens de correio o programa deve monitorar.

   - Se você escolher **Correio da Microsoft (MAPI)** como o seu sistema de correio eletrônico corporativo, estas são as suas opções:

     – **Todo novo correio.** Selecione este botão para que o VShield procure vírus nos arquivos anexados em cada mensagem de correio eletrônico ao chegar na sua caixa de correio MAPI ou via outros serviços MAPI. Escolha esta opção se você receber correio eletrônico de mais de uma origem — através do seu sistema corporativo de correio eletrônico e um cliente POP-3 ou SMTP, por exemplo — ou se o seu sistema de correio entregar correspondência em mais de uma caixa de correio.

     IMPORTANTE: Como esta opção informa ao VShield para examinar anexos de arquivos somente em novas mensagens de correio eletrônico, o programa não encontrará um vírus em mensagens de correio já armazenadas no seu computador ou servidor de correio. Para assegurar uma proteção ampla, execute uma operação de varredura completa com o componente Varredura de Correio Eletrônico do VirusScan. Veja o Capítulo 7, "Usando ferramentas de varredura Especializadas," para obter mais detalhes.

– **Selecionar Pasta.** Selecione este botão para designar uma pasta específica para ser examinada pelo VShield. Escolha essa opção se o seu sistema de correio eletrônico entregar as suas mensagens em um local determinado de um servidor de correio ou no seu computador. Em seguida, clique **Procurar** para abrir uma caixa de diálogo na qual você pode escolher a pasta que será examinada pelo VShield.

  Se já tiver sido estabelecida a conexão com o seu sistema de correio eletrônico, a caixa de diálogo lhe mostrará as caixas de correio disponíveis e outras pastas para este sistema. Caso ainda não tenha se conectado ao seu sistema de correio, o VShield tentará usar o seu perfil MAPI padrão MAPI para fazê-lo. Escolha a pasta que o VShield deverá examinar, em seguida clique em **OK** para fechar a caixa de diálogo.

- Se você escolher **Lotus cc:Mail** como o seu sistema de correio eletrônico corporativo, precisará informar ao VShield a freqüência na qual deve examinar a Caixa de Entrada do cc:Mail (Figura 4-17).
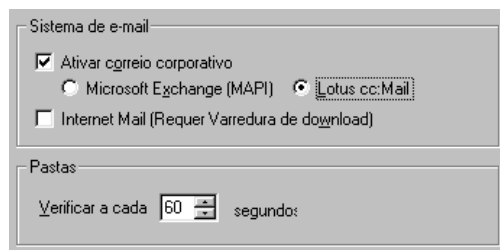
Figura 4-17. Página Detecção com a opção cc:Mail escolhida

Na área **Pastas**, digite o número de segundos que o VShield aguardará antes de procurar vírus. Como padrão, o programa verifica uma vez por minuto. Certifique-se de ter definido um intervalo menor do que do que o configurado para receber correio eletrônico, a fim de que o VShield possa detectar vírus antes que cheguem ao seu computador.

4. Especifique os tipos de anexos de correio eletrônico que devem ser examinados pelo VShield. Você pode

   - **Examinar arquivos compactados.** Marque a caixa de seleção **Arquivos compactados** para que a Varredura de Correio Eletrônico procure vírus em arquivos compactados com estes formatos: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Embora esse procedimento ofereça melhor proteção, a varredura de arquivos compactados pode alongar mais cada operação, especialmente quando for processado um grande volume de correio.

   - **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Portanto, você pode reduzir a abrangência das operações de varredura a esses arquivos mais suscetíveis a infecções por vírus, a fim de acelerar as operações de varredura quando tiver um grande volume de correio a processar.

     Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou determinar as extensões de nomes de arquivos que o VShield examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (Figura 4-18).
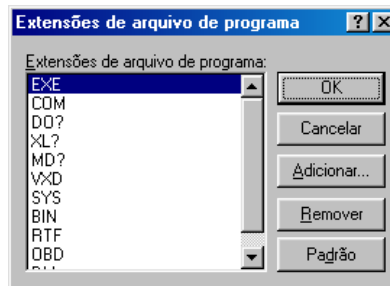
Figura 4-18. Caixa de diálogo Extensões de arquivo de programa

Como padrão, o VShield procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .OBD,.VXD, .MD? e .DLL. Os arquivos com as extensões.DO?, .XL?, .RTF, .MD? e .OBD pertencem ao Microsoft Office, todos esses podem ser infectados por vírus de macros. O ? é um curinga que ativa o VShield para examinar arquivos de documentos e de modelos.

– Para adicioná-las à lista, clique em **Adicionar**, em seguida, digite as extensões que o VShield deverá examinar na caixa de diálogo mostrada.

– Para remover uma extensão da lista, selecione-a, em seguida, clique em **Remover**.

– Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

- **Examinar todos os anexos.** Para que o VShield examine os anexos recebidos junto com as mensagens de correio eletrônico, com qualquer extensão, selecione o botão **Todos os anexos**. Isso pode reduzir a velocidade de processamento do correio eletrônico, se você receber um volume grande de correio eletrônico, mas assegura que as suas mensagens não estarão infectadas.

5. Clique na guia Ação para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura de Correio Eletrônico, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Ação

Quando o VShield detecta um vírus, poderá lhe perguntar o que deve fazer com o arquivo infectado, ou atuar automaticamente utilizando uma ação predeterminada. Use a página de propriedades Ação para especificar quais opções de ação o VShield deve lhe propor ao encontrar um vírus ou quais ações o programa deve realizar automaticamente.

Siga estas etapas:

1. Clique na guia Ação no módulo Varredura de Correio Eletrônico para exibir a página de propriedades correta (Figura 4-19).

Figura 4-19. Caixa de diálogo Propriedades da Varredura de Correio Eletrônico – página Ação

2. Escolha uma ação na lista **Quando um vírus for encontrado**. A área abaixo da lista será alterada para mostrar as opções adicionais para cada uma delas. Estas são as opções:

   - **Solicitar ação ao usuário.** Escolha esta opção se você quiser que o VShield o consulte sobre o que fazer quando encontrar um vírus — o programa exibirá uma mensagem de alerta e proporá opções de ação possíveis. Escolha as opções que você deseja ver na mensagem de alerta:

     – **Excluir arquivo.** Esta opção informa ao VShield para excluir o arquivo infectado imediatamente. Contudo, o VShield preservará a mensagem de correio eletrônico na qual o arquivo estava contido.

     – **Mover arquivo.** Esta opção informa ao VShield para mover o arquivo infectado para um diretório de quarentena pré-selecionado.

     – **Continuar a varredura.** Esta opção informa ao VShield para continuar com a varredura, mas não atuar de qualquer outra maneira. Se as opções de relatório estiverem ativadas, o VShield incluirá a ocorrência no arquivo de registro.

   - **Mover arquivos infectados para uma pasta**. Escolha esta opção para que o VShield mova os arquivos infectados para um diretório de quarentena assim que os encontrar. Como padrão, o VShield move esses arquivos para uma pasta chamada INFECTADO.

     Se você usar um sistema de correio eletrônico corporativo, o VShield criará uma pasta INFECTADO no servidor de correio da rede. Não é possível especificar uma pasta diferente nem alterar o nome da pasta. Contudo, dependendo do tipo do seu acesso ao servidor de correio através do cliente de correio eletrônico, você poderá ver ou excluir o arquivo nessa pasta.

     Se for utilizado um cliente de correio da Internet, o VShield criará uma pasta INFECTADO no nível raiz da unidade na qual é feito download do seu correio. Por exemplo, se a “caixa de entrada” do seu cliente de correio estiver na unidade D: e o VShield encontrar um anexo infectado no seu correio eletrônico, o programa criará o diretório D:\INFECTADO e copiará nele o arquivo.

Você pode alterar o nome e a localização da pasta na qual o VShield coloca o correio da Internet infectado, mas para fazê-lo, é necessário alternar para a Varredura de Download e clicar na guia Ação desse módulo. Veja “Escolhendo opções de Ação” na página 126 para obter mais detalhes.

- **Excluir arquivos infectados.** Escolha esta opção para que o VShield exclua imediatamente os arquivos infectados detectados. Certifique-se de ter ativado o recurso de relatório para que você tenha um registro de quais arquivos o VShield excluiu. Será necessário restaurar os anexos excluídos a partir de cópias de backup. Veja o “Escolhendo opções de Relatório” na página 121 para obter mais detalhes.

- **Continuar a varredura.** Escolha esta opção para que VShield continue a varredura, mas não atue de qualquer outra maneira. Se as opções de relatório também forem ativadas, (veja “Escolhendo opções de Relatório” na página 121 para obter mais detalhes), o programa registrará os nomes dos vírus encontrados e os nomes dos arquivos infectados, para que você possa excluí-los na próxima oportunidade.

3. Clique na guia Alerta para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura de Correio Eletrônico, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Alerta

Após configurá-lo com as opções de ação desejadas, o VShield irá procurar vírus na entrada de correio eletrônico e remover automaticamente os vírus encontrados, não sendo necessárias outras intervenções. Contudo, se o VShield deve lhe avisar imediatamente após encontrar um vírus, a fim de que seja realizada a ação necessária, é possível configurá-lo para enviar uma mensagem de alerta para você ou outras pessoas de várias maneiras. Use a página de propriedades Alerta para escolher quais métodos serão utilizados.

Siga estas etapas:

1. Clique na guia Alerta no módulo Varredura de Correio Eletrônico para exibir a página de propriedades correta (Figura 4-20).
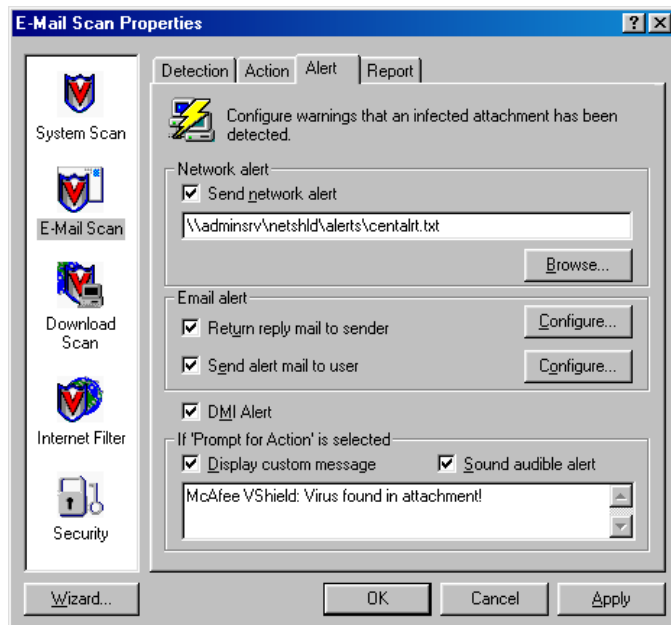
Figura 4-20. Caixa de diálogo Propriedades da Varredura de Correio Eletrônico – página Alerta

2. Para informar ao VShield que envie uma mensagem de alerta a um servidor que esteja executando o NetShield , uma solução antivírus com base em servidor da Network Associates, marque a caixa de verificação **Enviar alerta de rede**, em seguida, digite o caminho para a pasta de alertas do NetShield na sua rede ou clique em **Procurar** para localizar a pasta correta.

NOTA: A pasta escolhida deve conter o CENTALRT.TXT, o arquivo Alerta Centralizado do NetShield. Esse programa coleta as mensagens de alerta do VShield e de outros softwares da Network Associates, em seguida, passa-os para os administradores de rede para que realizem as ações necessárias. Para saber mais sobre o Alerta Centralizado, veja o *Guia do Usuário* do NetShield.

3. Para enviar uma mensagem de alerta para uma pessoa que lhe enviou o anexo de correio eletrônico infectado, marque a caixa de seleção **Enviar resposta de correio ao remetente**. Em seguida, você pode compor uma resposta padrão para ser enviada. Siga estas etapas:

   a. Clique em **Configurar** para abrir um formulário de mensagem de correio padrão.

   b. Preencha a linha do assunto, em seguida, adicione os comentários que quiser no corpo da mensagem, abaixo de uma nota sobre a infecção que o VShield fornecerá. Podem ser adicionados até 1024 caracteres de texto.

   c. Para enviar uma cópia dessa mensagem para outra pessoa, digite um endereço de correio eletrônico na caixa de texto rotulada com **Cc:**, ou clique em **Cc:** para escolher um destinatário na lista de endereços de seu sistema de correio eletrônico.

   NOTA: Para localizar um endereço de correio eletrônico no seu diretório de usuários do sistema de correio, você deve armazenar informações sobre endereços em um diretório de usuários, banco de dados ou agenda de endereços compatíveis com MAPI, ou ainda em um diretório do Lotus cc:Mail equivalente. Se ainda não estiver conectado ao seu sistema de correio eletrônico, o VShield tentará usar o seu perfil MAPI padrão para conectar-se aos sistemas de correio compatíveis com essa interface ou lhe pedirá para fornecer um nome de usuário, uma senha e um caminho para a caixa de correio do Lotus cc:Mail. Digite as informações necessárias para o VShield, em seguida clique em **OK** para continuar.

   d. Clique em **OK** para salvar a mensagem.

Ao detectar um vírus, o VShield enviará uma cópia desta mensagem para cada pessoa que lhe envia correio eletrônico com anexo infectado. O programa preenche o endereço do destinatário com as informações encontradas no cabeçalho da mensagem original, e identifica o vírus e o arquivo infectado na área imediatamente abaixo da linha do assunto. Se o recurso de relatório estiver ativado, o VShield também registrará cada ocorrência quando enviar uma mensagem de alerta.

4. Para enviar uma mensagem de correio eletrônico a fim de avisar as pessoas sobre um anexo infectado, marque a caixa de verificação **Enviar mensagem de alerta para o usuário**. Em seguida, componha uma resposta padrão para enviá-la a um ou mais destinatários — um administrador de rede, por exemplo — sempre que o VShield detectar um anexo de correio eletrônico infectado. Siga estas etapas:

   a. Clique em **Configurar** para abrir um formulário de mensagem de correio padrão.

   b. Digite um endereço de correio eletrônico na caixa de texto rotulada **Para:**, ou clique em **Para:** para escolher um destinatário na lista de endereços de seu sistema de correio eletrônico. Repita esse procedimento na caixa de texto rotulada com **Cc:** para enviar uma cópia da mensagem para outra pessoa.

   NOTA: Para localizar um endereço de correio eletrônico no diretório de usuários do seu sistema de correio, você deve armazenar informações sobre endereços em um diretório de usuários, banco de dados ou agenda de endereços compatível com MAPI, ou em um diretório equivalente do Lotus cc:Mail. Se ainda não tiver sido estabelecida a sua conexão com o sistema de correio eletrônico, o VShield lhe pedirá que escolha um perfil de usuário que o programa possa usar para conectar-se a sistemas de correio compatíveis com MAPI, ou que forneça um nome de usuário, senha e caminho para a sua caixa de correio do Lotus cc:Mail. Digite as informações necessárias para o VShield, em seguida clique em **OK** para continuar.

   ---

   c. Preencha a linha do assunto, em seguida, acrescente os comentários desejados no corpo da mensagem, abaixo do aviso de infecção. Podem ser adicionados até 1024 caracteres de texto.

   d. Clique em **OK** para salvar a mensagem.

   Ao detectar um vírus, o VShield envia uma cópia desta mensagem para cada um dos endereços digitados na Etapa b. O programa adiciona informações para identificar o vírus e o arquivo infectado, na área imediatamente abaixo da linha do assunto. Se o recurso de relatório estiver ativado, o VShield também registrará cada ocorrência quando enviar uma mensagem de alerta.

5. Para que o VShield envie mensagens de alerta sobre vírus através da interface de componente DMI para a área de trabalho e para os aplicativos de gerenciamento que estejam sendo executados na rede, marque a caixa de verificação **Alerta DMI**.

NOTA: A Desktop Management Interface é um padrão para comunicação de solicitações de gerenciamento e informações sobre alertas entre componentes de hardware e software armazenados em ou conectados a computadores de mesa, e os aplicativos utilizados para gerenciá-los. Para saber mais sobre a utilização desse método de alerta, consulte o administrador da rede.

6. Se você escolher **Solicitar ação ao usuário** como a sua opção na página Ação (veja "Escolhendo opções de Ação" na página 115 para obter mais detalhes), também poderá informar ao VShield que emita um sinal sonoro e exiba uma mensagem personalizada ao encontrar um vírus. Para fazer isso, marque a caixa de verificação **Exibir mensagem personalizada** em seguida, digite a mensagem que aparecerá na caixa de texto mostrada — pode ser digitada uma mensagem com 225 caracteres, no máximo. Depois, marque a caixa de verificação **Soar alerta audível**.

7. Clique na guia Relatório para escolher as opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura de Correio Eletrônico, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Relatório

O módulo Varredura de Correio Eletrônico do VShield contém uma lista com as configurações atuais e resume todas as ações efetuadas, durante as operações de varredura, em um arquivo de registro chamado WEBEMAIL.TXT. O VShield poderá gravar o registro nesse arquivo ou usar um arquivo de texto criado com qualquer editor de texto. Esse arquivo de registro pode ser aberto e impresso para revisão posterior em qualquer editor de texto.

O arquivo WEBEMAIL.TXT pode servir como uma importante ferramenta de gerenciamento para controlar a atividade de vírus no sistema e anotar quais configurações foram usadas, a fim de detectar e atuar contra as infecções encontradas pelo VShield. Você também pode utilizar os relatórios de ocorrências registrados no arquivo para determinar quais arquivos é necessário substituir a partir de cópias de backup, examinar na pasta de quarentena ou excluir do seu computador. Use a página de propriedades Relatório para determinar quais informações o VShield incluirá no arquivo de registro.

Para configurar o VShield a fim de registrar suas ações em um arquivo de registro, siga estas etapas:

1. Clique na guia Relatório do módulo Varredura de Correio Eletrônico para exibir a página de propriedades correta (veja a Figura 4-21).

Figura 4-21. Caixa de diálogo Propriedades da Varredura de Correio Eletrônico – página Relatório

2. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, o VShield grava as informações sobre registro no WEBEMAIL.TXT, no diretório de programa do VirusScan. Você pode digitar um nome e um caminho diferentes na caixa de texto mostrada, ou clique em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

3. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o VShield limita o tamanho de arquivo em 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, o VShield apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

4. Marque as caixas de verificação correspondentes às informações que o VShield deverá incluir no arquivo de registro. Você pode optar por gravar estas informações:

   - **Detecção de vírus.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados, encontrados quando o programa examinou o seu correio eletrônico.
   - **Eliminação do arquivo infectado.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados excluídos, quando o programa verificou o seu correio eletrônico.
   - **Movimentação do arquivo infectado.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados que ele moveu para o diretório de quarentena.
   - **Configurações da sessão.** Marque esta caixa de verificação para que o VShield faça uma lista das opções escolhidas na caixa de diálogo Propriedades da Varredura de Correio Eletrônico, para cada sessão de varredura.
   - **Resumo da sessão.** Marque esta caixa de verificação para que o VShield faça um resumo das suas ações durante cada sessão de varredura. As informações do resumo incluem o número de arquivos examinados pelo VShield, o número e o tipo de vírus detectados, o número de arquivos movidos ou excluídos, e outras informações.

5. Clique em uma guia diferente para alterar qualquer uma das configurações da Varredura de Correio Eletrônico ou clique em um dos ícones na lateral da caixa de diálogo Propriedades da Varredura de Correio Eletrônico para escolher opções para outro módulo.

   Para salvar as alterações no módulo Varredura de Correio Eletrônico sem fechar a caixa de diálogo, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Configurando o módulo Varredura de Download

O módulo Varredura de Download do VShield pode examinar arquivos obtidos por download na Internet quando você visita sites da web, sites de FTP e outros sites da Internet. É nesse módulo também onde são definidas as opções que serão usadas para atuar contra anexos de arquivos infectados recebidos através de programas de clientes POP-3 ou SMTP de correio eletrônico, como Eudora, Netscape Mail ou Microsoft Outlook Express. Para ativar esta função, você também deve escolher um sistema de correio adequado na página Detecção do módulo Varredura de Correio Eletrônico. Veja "Escolhendo opções de Detecção" na página 109 para obter mais detalhes.

Para configurar o VShield a fim de que o programa examine arquivos obtidos por download, clique no ícone da Varredura de Download, no lado direito da caixa de diálogo Propriedades do VShield a fim de exibir as páginas de propriedades para esse módulo. As seções seguintes descrevem as opções.

Escolhendo opções de Detecção

O VShield supõe que você deseja procurar vírus sempre que fizer download de um arquivo suscetível a infecção por vírus, na Internet (veja Figura 4-22). Estas opções padrão fornecem uma segurança excelente, mas o seu ambiente pode necessitar de configurações diferentes.
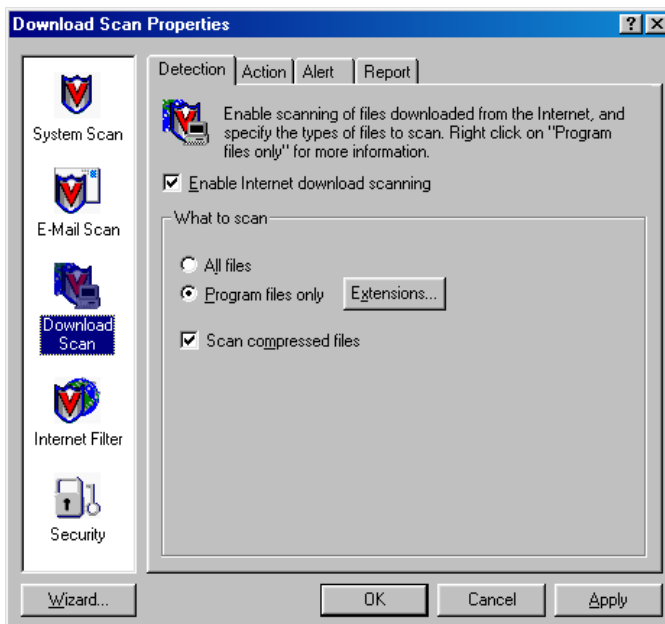
Figura 4-22. Caixa de diálogo Propriedades da Varredura de Download - página Detecção

Para modificar essas configurações, verifique se a caixa de verificação Ativar a Varredura de Download da Internet está selecionada, depois siga as etapas abaixo:

1. Especifique os tipos de arquivo que o VShield examinará. Você pode

   - **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Contudo, você pode reduzir seguramente a abrangência das operações de varredura para os arquivos mais suscetíveis a infecções por vírus, a fim de acelerar o download de arquivos, particularmente os grandes ou em grupo numeroso. Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou determinar as extensões de nomes de arquivos que o VShield examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (Figura 4-23).
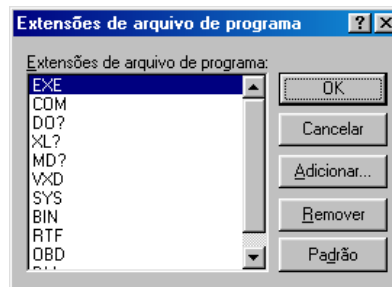
Figura 4-23. Caixa de diálogo Extensões de arquivo de programa

Como padrão, o VShield procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .OBD,.VXD, .MD? e .DLL. Os arquivos com as extensões.DO?, .XL?, .RTF, .MD? e .OBD pertencem ao Microsoft Office, sendo que todos podem ser infectados por vírus de macros. O ? é um curinga que possibilita ao VShield examinar arquivos de modelos e de documentos.

   – Para adicioná-las à lista, clique em **Adicionar**, em seguida, digite as extensões que o VShield deverá examinar na caixa de diálogo mostrada.

   – Para remover uma extensão da lista, selecione-a, em seguida, clique em **Remover**.

   – Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

- **Examinar todos os arquivos.** Para que o VShield examine os arquivos obtidos por download, com qualquer extensão, selecione o botão **Todos os arquivos**. Isto poderá ralentar as operações de download, mas irá assegurar que o sistema estará sem vírus.

- **Examinar arquivos compactados.** Marque a caixa de seleção **Arquivos compactados** para que a Varredura de Download procure vírus em arquivos compactados nos formatos: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Embora esse procedimento lhe ofereça uma melhor proteção, a varredura de arquivos compactados ao fazer o download pode aumentar o tempo de descarregamento.

2. Clique na guia Ação para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura de Download, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Ação

Quando o VShield detecta um vírus, poderá lhe perguntar o que deve fazer com o arquivo infectado ou atuar automaticamente utilizando uma ação predeterminada. Use a página de propriedades Ação para especificar quais opções de ação o VShield deve lhe propor ao encontrar um vírus ou quais ações o programa deve realizar automaticamente.

Siga estas etapas:

1. Clique na guia Ação no módulo Varredura de Download para exibir a página de propriedades correta (Figura 4-24).

Figura 4-24. Caixa de diálogo Propriedades da Varredura de Download – página Ação

2. Escolha uma ação na lista **Quando um vírus for encontrado**. A área imediatamente abaixo da lista será alterada para mostrar as opções adicionais para cada uma delas. Estas são as opções:

   - **Solicitar ação ao usuário.** Escolha esta opção se o VShield lhe perguntar o que fazer quando encontrar um vírus — o programa exibirá uma mensagem de alerta e proporá opções de ação possíveis. Escolha as opções que você deseja ver na mensagem de alerta:

     – **Mover arquivo.** Esta opção informa ao VShield para mover o arquivo infectado para um diretório de quarentena de sua escolha.

     – **Excluir arquivo.** Esta opção informa ao VShield para excluir o arquivo infectado imediatamente.

– **Continuar a varredura.** Esta opção informa ao VShield para continuar com a varredura, mas não atuar de qualquer outra maneira. Se as opções de relatório estiverem ativadas, o VShield incluirá a ocorrência no arquivo de registro.

- **Mover arquivos infectados para uma pasta**. Escolha esta opção para que o VShield mova os arquivos infectados para um diretório de quarentena assim que encontrá-los. Como padrão, o VShield move esses arquivos para uma pasta chamada INFECTADO, criada no nível raiz do disco rígido, na qual você salva arquivos obtidos por download.

  Por exemplo, se o VShield encontrou um vírus em um arquivo cujo download foi colocado em E:\MEUS DOWNLOADS e você especificou INFECTADO como o diretório de quarentena, o VShield copiará o arquivo para E:\INFECTADO.

  Você pode digitar um nome e um caminho diferentes na caixa de texto ou clicar em **Procurar** para localizar uma pasta adequada no disco rígido.

- **Excluir arquivos infectados.** Escolha esta opção para que o VShield exclua os arquivos infectados, obtidos por download. Certifique-se de ter ativado o recurso de relatório para que você tenha um registro de quais arquivos o VShield excluiu.

- **Continuar a varredura.** Escolha esta opção para que o VShield continue a varredura, mas não atue de qualquer outra maneira. Se as opções de relatório também forem ativadas, (veja "Escolhendo opções de Relatório" na página 131 para obter mais detalhes), o programa registrará os nomes dos vírus encontrados e os nomes dos arquivos infectados, para que você possa excluí-los na próxima oportunidade.

3. Clique na guia Alerta para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura de Download, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Alerta

Após configurá-lo com as opções de ação desejadas, o VShield irá procurar vírus e removerá aqueles encontrados nos arquivos obtidos por download, sem que outras intervenções sejam necessárias. Contudo, se você quiser que o VShield lhe avise imediatamente após encontrar um vírus, para tomar a atitude adequada, configure-o de modo a enviar uma mensagem de alerta para você ou outras pessoas de várias maneiras. Use a página de propriedades Alerta para escolher quais métodos serão utilizados.

Siga estas etapas:

1. Clique na guia Alerta no módulo Varredura de Download para exibir a página de propriedades correta (veja Figura 4-25).
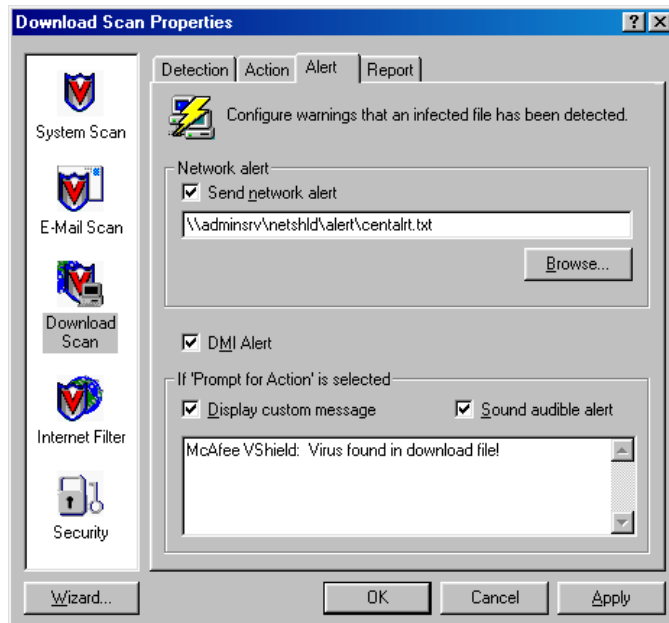
Figura 4-25. Caixa de diálogo Propriedades da Varredura de Download – página Alerta

2. Para informar ao VShield que envie uma mensagem de alerta a um servidor que esteja executando o NetShield , uma solução antivírus com base em servidor da Network Associates, marque a caixa de verificação **Enviar alerta de rede**, em seguida, digite o caminho para a pasta de alertas do NetShield na sua rede ou clique em **Procurar** para localizar a pasta correta.

   ❐ **NOTA:** A pasta escolhida deve conter o CENTALRT.TXT, o arquivo Alerta Centralizado do NetShield. Esse programa coleta as mensagens de alerta do VShield e de outros softwares da Network Associates, em seguida, passa-os para os administradores de rede para que realizem as ações necessárias. Para saber mais sobre o Alerta Centralizado, veja o *Guia do Usuário* do NetShield.

3. Para que o VShield envie mensagens de alerta sobre vírus através da interface de componente DMI para a área de trabalho e para os aplicativos de gerenciamento que estejam sendo executados na rede, marque a caixa de verificação **Alerta DMI**.

   ❐ **NOTA:** A Desktop Management Interface é um padrão para comunicação de solicitações de gerenciamento e informações sobre alertas entre componentes de hardware e software armazenados em ou conectados a computadores de mesa, e os aplicativos utilizados para gerenciá-los. Para saber mais sobre a utilização desse método de alerta, consulte o administrador da rede.

4. Se você escolher **Solicitar ação ao usuário** como a sua opção na página Ação (veja “Escolhendo opções de Ação” na página 126 para obter mais detalhes), também poderá informar ao VShield que emita um sinal sonoro e exiba uma mensagem personalizada ao encontrar um vírus. Para fazê-lo, marque a caixa de seleção **Exibir mensagem personalizada** em seguida digite a mensagem desejada para vê-la na caixa de texto mostrada — a mensagem pode conter 225 caracteres no máximo. Depois, marque a caixa de verificação **Soar alerta audível**.

5. Clique na guia Relatório para escolher as opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades da Varredura de Download, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

   ❐ **NOTA:** O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Relatório

O módulo Varredura de Download do VShield cria uma lista com as configurações atuais e resume todas as ações efetuadas, durante as operações de varredura, em um arquivo de registro chamado WEBINET.TXT. O VShield poderá gravar o registro nesse arquivo ou usar um arquivo de texto que você criou com qualquer editor de texto. Esse arquivo de registro pode ser aberto e impresso para revisão posterior em qualquer editor de texto. Use a página de propriedades Relatório para determinar quais informações o VShield incluirá no arquivo de registro.

Para configurar o VShield a fim de registrar suas ações em um arquivo de registro, siga estas etapas:

1. Clique na guia Relatório do módulo Varredura de Download para exibir a página de propriedades correta (Figura 4-26).
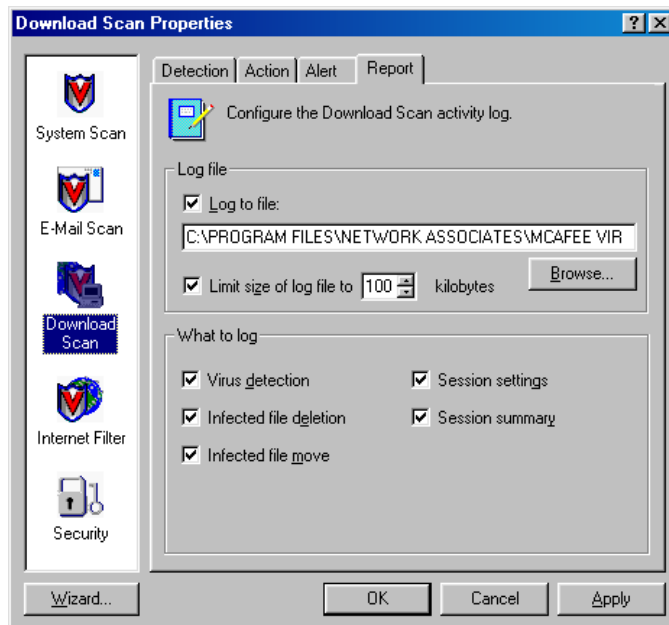
Figura 4-26. Caixa de diálogo Propriedades da Varredura de Download – página Relatório

2. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, o VShield grava as informações de registro no arquivo WEBINET.TXT no diretório de programa do VirusScan. Você pode digitar um nome e um caminho diferentes na caixa de texto mostrada, ou clicar em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

3. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o VShield limita o tamanho de arquivo em 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, o VShield apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

4. Marque as caixas de seleção correspondentes às informações que o VShield deverá incluir no arquivo de registro. Você pode escolher gravar qualquer uma destas informações:

   - **Detecção de vírus.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados, encontrados durante o download.

   - **Eliminação do arquivo infectado.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados durante o download.

   - **Movimentação do arquivo infectado.** Marque esta caixa de verificação para que o VShield anote o número de arquivos infectados que ele moveu para o diretório de quarentena.

   - **Configurações da sessão.** Marque esta caixa de seleção para que o VShield faça uma lista das opções escolhidas na caixa de diálogo Propriedades da Varredura de Download para cada sessão de varredura.

   - **Resumo da sessão.** Marque esta caixa de verificação para que o VShield faça um resumo das suas ações durante cada sessão de varredura. As informações do resumo incluem o número de arquivos examinados pelo VShield, o número e o tipo de vírus detectados, o número de arquivos movidos ou excluídos, e outras informações.

5. Clique em uma guia diferente para alterar as configurações da Varredura de Download ou clique em um dos ícones na lateral da caixa de diálogo Propriedades da Varredura de Download para escolher opções para outros módulos.

   Para salvar as alterações no módulo Varredura de Download sem fechar a caixa de diálogo, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Configurando o módulo Filtro de Internet

Embora os objetos Java e ActiveX incluam proteções que se destinam a impedir danos ao seu sistema de computador, programadores mal-intencionados desenvolveram objetos que exploram os recursos Java ou ActiveX mais secretos para causar várias formas de prejuízos ao seu sistema.

Objetos perigosos como estes, freqüentemente, podem esconder-se em sites da web até que você os visite e os transfira para o seu sistema, geralmente sem perceber que eles existem. A maioria dos softwares de navegação incluem um recurso que permite bloquear miniaplicativos Java e controles ActiveX, ou ativar recursos de segurança que autenticam objetos, antes que sejam descarregados no sistema. Mas essas abordagens podem impedi-lo de beneficiar-se dos recursos interativos dos sites da Web que você visita, pois bloqueiam todos os objetos perigosos ou não, indiscriminadamente.

O VShield permite um tratamento mais criterioso. Esse programa utiliza um banco de dados atualizado de objetos conhecidos por causar danos a classes Java e controles ActiveX de tela, encontrados durante a navegação.

Para configurar o VShield a fim de que bloqueie objetos destrutivos e filtre sites da Internet perigosos, clique no ícone do Filtro de Internet, no lado esquerdo da caixa de diálogo Propriedades do VShield para exibir as páginas de propriedades para esse módulo. As seções seguintes descrevem as opções.

Escolhendo opções de Detecção

O VShield bloqueia inicialmente os objetos destrutivos e os sites contidos nas listagens de seu banco de dados, para evitar que você os encontre (Figura 4-27).
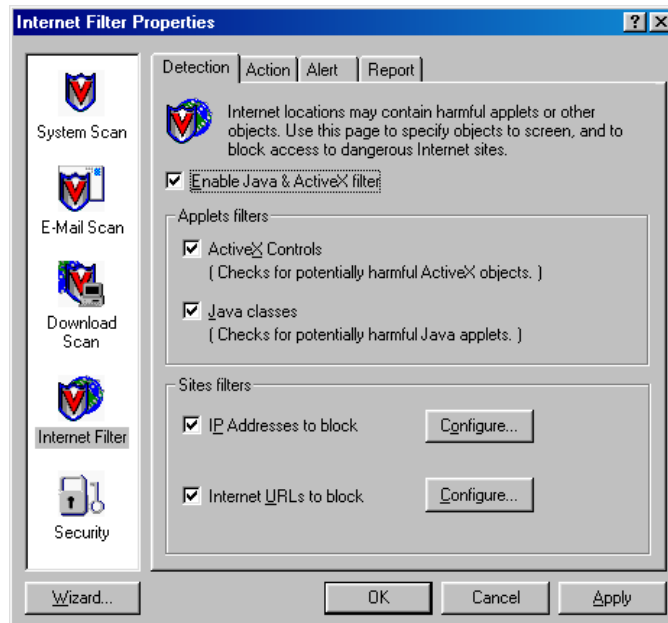
Figura 4-27. Filtro de Internet Propriedades - página Detecção

Para alterar essas opções padrão, verifique se a caixa de verificação Ativar filtro de Java e ActiveX está marcada, depois siga estas etapas:

1. Informe ao VShield quais objetos devem ser filtrados. Estas são as opções:

   - **Controles ActiveX.** Marque esta caixa de verificação para que o VShield procure e bloqueie controles ActiveX ou .OCX destrutivos.

   - **Classes Java.** Marque esta caixa de verificação para que o VShield procure e bloqueie classes Java destrutivas, ou miniaplicativos escritos em Java.

O VShield compara os objetos encontrados quando você visita os sites da Internet, às listas de características de objetos conhecidos por causar danos do seu banco de dados interno. Quando encontra uma coincidência, o VShield poderá alertá-lo e deixar que você decida o que fazer, ou impedir automaticamente que seja feito download do objeto. Veja “Escolhendo opções de Ação” na página 138 para obter mais detalhes.

2. Informe ao VShield quais sites filtrar. O programa usa uma lista de sites de Internet perigosos para decidir quais o navegador será impedido de visitar. Você pode ativar esta função e acrescentar sites à lista de “banidos” de duas maneiras:

   - **Endereços IP a serem bloqueados.** Marque esta caixa de seleção para informar ao VShield que identifique os sites da Internet perigosos usando os seus endereços Internet Protocol (IP). Para ver ou especificar quais sites o VShield deve banir, clique em **Configurar**, para abrir a caixa de diálogo Endereços IP banidos (Figura 4-28).
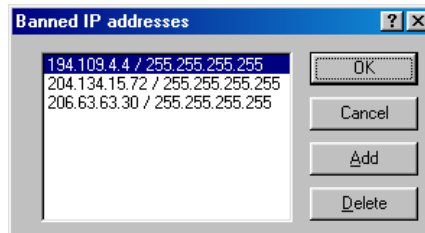
Figura 4-28. Caixa de diálogo Endereços IP banidos

Os endereços de Protocolo Internet consistem de quatro grupos de três números cada, formatadas da seguinte maneira:

123.123.123.123

Cada grupo de números pode variar entre zero e 255. O VShield pode utilizá-lo para identificar um computador ou rede específica na Internet e impedir que o seu navegador se conecte a este local. Na Figura 4-28, cada endereço contém dois conjuntos de números IP. O primeiro é o endereço do domínio do site banido — o número que é usado para localizá-lo na Internet — segundo é a “máscara de sub-rede”.

Uma máscara de sub-rede é um modo de “remapear” um intervalo de endereços de computadores em uma rede interna. O VShield coloca na lista uma máscara de sub-rede padrão cujo número é 255.255.255.255. Na maioria dos casos, você não precisará alterá-la, mas se souber de um nó de rede específico no site visitado que poderá causar problema, será necessário digitar uma máscara de sub-rede para preservar o seu acesso a outras máquinas neste site.

– Para adicionar entradas na lista de banidos, clique em **Adicionar**, em seguida, digite os endereços que o Vshield deve bloquear, na caixa de diálogo mostrada (Figura 4-29).
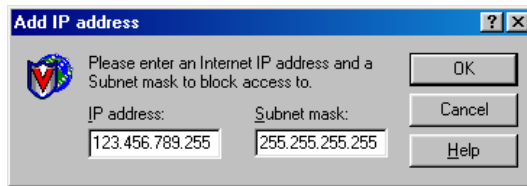
Figura 4-29. Caixa de diálogo Adicionar endereço IP

Certifique-se de ter digitado cada endereço com atenção, na forma correta. Se você souber o valor da máscara de sub-rede do site que deseja evitar, digite-o na caixa de texto abaixo. Caso contrário, mantenha o valor padrão mostrado. Clique em **OK** para salvar o endereço e retornar à caixa de diálogo Endereços IP banidos. Para adicionar outro endereço na lista, repita essas etapas.

– Para remover um endereço da lista de banidos, selecione-o e clique em **Excluir**.

Ao terminar de editar a lista, clique em **OK** para salvar as alterações e retornar à caixa de diálogo Propriedades do Filtro de Internet. Clique em **Cancelar** para fechar a caixa de diálogo sem salvar as alterações.

- **URLs da Internet a serem bloqueados.** Marque esta caixa de seleção para informar o VShield para identificar os sites da Internet perigosos usando a designação de Uniform Resource Locator. Para ver ou escolher quais endereços o VShield deve banir, clique em **Configurar** para abrir a caixa de diálogo URLs banidos (Figura 4-30 na página 137).
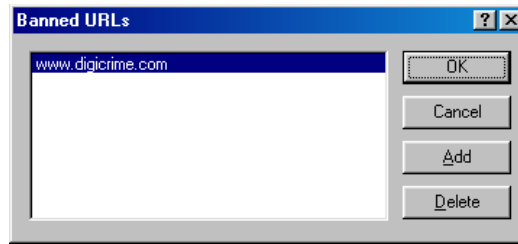
Figura 4-30. Caixa de diálogo URLs banidos

Algumas vezes, se for utilizado de modo intercambiável com o "nome do domínio" ou o "nome do host", um URL especifica o nome e a localização do computador na Internet, normalmente junto com o "protocolo de transporte" que você deseja usar para solicitar um recurso desse computador. Um URL completo para um site da Web, por exemplo, teria a seguinte forma:

http://www.dominioperigoso.com

O URL completo informa ao seu navegador para solicitar recursos através do HyperText Transport Protocol (“http://”) em um computador chamado “www” em uma rede chamada “dominioperigoso.com”. Outros protocolos de transporte incluem “ftp://” e “gopher://”. O sistema Domain Name Server(DNS) da Internet converte os URLs em endereços IP corretos usando um banco de dados atualizado, centralizado e com referências cruzadas.

– Para adicionar entradas na lista de banidos, clique em **Adicionar**, em seguida, digite os endereços que o Vshield deve bloquear, na caixa de diálogo mostrada (Figura 4-31).
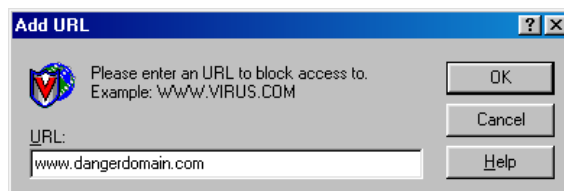
Figura 4-31. Caixa de diálogo Adicionar URL

Certifique-se de ter digitado cada endereço com atenção, na forma correta. Para banir um site da web, você pode digitar *somente o nome do domínio*; o VShield assumirá que este é o HyperText Transport Protocol. Clique em **OK** para salvar o endereço e retornar à caixa de diálogo Endereços IP banidos. Para adicionar outro endereço na lista, repita essas etapas.

– Para remover um endereço da lista de banidos, selecione-o e clique em **Excluir**.

Ao terminar de editar a lista, clique em **OK** para salvar as alterações e retornar à caixa de diálogo Propriedades do Filtro de Internet. Clique em **Cancelar** para fechar a caixa de diálogo sem salvar as alterações.

3. Clique na guia Ação para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do Filtro de Internet, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Ação

Quando o VShield encontra um objeto perigoso ou um site banido, o programa atuará perguntando-lhe se deve bloquear o objeto ou site ou o bloqueia automaticamente. Use a página de propriedades Ação para especificar qual será a atuação do VShield.

Como padrão, o VShield aguarda a sua decisão sobre o que fazer (Figura 4-32 na página 139).

Figura 4-32. Caixa de diálogo Propriedades do Filtro de Internet – página Ação

Escolha uma ação na lista **Quando for encontrado um objeto potencialmente destrutivo**. Estas são as opções:

- **Solicitar ação ao usuário.** Escolha esta opção para que o VShield lhe pergunte se deve bloquear um objeto ou site destrutivo, ou permitir o acesso a ele.

- **Negar acesso a objetos.** Escolha esta opção para que o VShield bloqueie os objetos ou sites destrutivos automaticamente. O programa fará isso com base no conteúdo do seu banco de dados, além de qualquer outra informação que você forneça sobre o site. Veja “Escolhendo opções de Detecção” na página 134 para obter mais detalhes.

Clique na guia Alerta para escolher opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do Filtro de Internet, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Alerta

Após configurá-lo com as opções de ação desejadas, o VShield irá procurar e bloquear objetos e sites da Internet destrutivos, sem necessitar de mais intervenções. Contudo, se você quiser que o VShield lhe informe imediatamente após encontrar um desses objetos ou sites, para que você possa atuar adequadamente, o programa pode ser configurado para enviar uma mensagem de alerta para você ou outras pessoas de várias maneiras. Use a página de propriedades de Alerta para escolher quais métodos devem ser utilizados.

Siga estas etapas:

1. Clique na guia Alerta no módulo Filtro de Internet para exibir a página de propriedades correta (Figura 4-33).
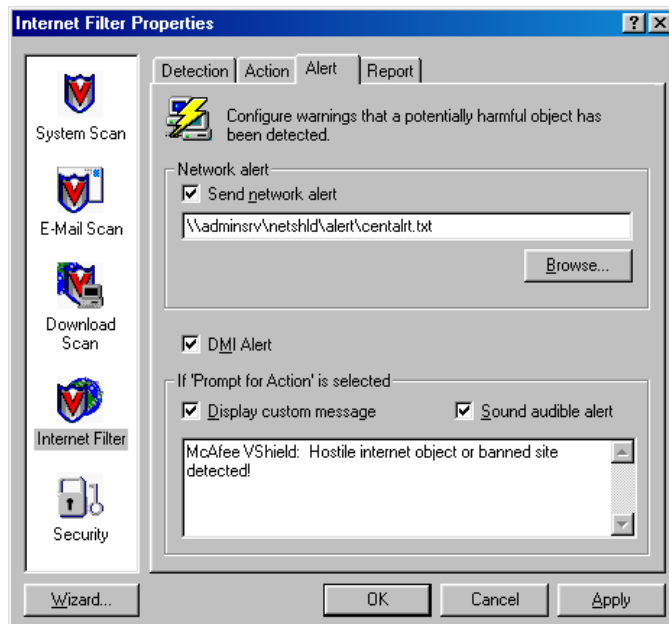
Figura 4-33. Caixa de diálogo Propriedades do Filtro de Internet – página Alerta

2. Para informar ao VShield que envie uma mensagem de alerta a um servidor que esteja executando o NetShield , uma solução antivírus com base em servidor da Network Associates, marque a caixa de verificação **Enviar alerta de rede**, em seguida, digite o caminho para a pasta de alertas do NetShield na sua rede ou clique em **Procurar** para localizar a pasta correta.

NOTA: A pasta escolhida deve conter o CENTALRT.TXT, o arquivo Alerta Centralizado do NetShield. Esse programa coleta as mensagens de alerta do VShield e de outros softwares da Network Associates, em seguida, passa-os para os administradores de rede para que realizem as ações necessárias. Para saber mais sobre o Alerta Centralizado, veja o *Guia do Usuário* do NetShield.

3. Para que o VShield envie mensagens de alerta sobre vírus através da interface de componente DMI para a área de trabalho e para os aplicativos de gerenciamento que estejam sendo executados na rede, marque a caixa de verificação **Alerta DMI**.

NOTA: A Desktop Management Interface é um padrão para comunicação de solicitações de gerenciamento e informações sobre alertas entre componentes de hardware e software armazenados em ou conectados a computadores de mesa, e os aplicativos utilizados para gerenciá-los. Para saber mais sobre a utilização desse método de alerta, consulte o administrador da rede.

4. Se você escolher **Solicitar ação ao usuário** como a sua opção na página Ação (veja “Escolhendo opções de Ação” na página 138 para obter mais detalhes), também poderá informar ao VShield que emita um sinal sonoro e exiba uma mensagem personalizada ao encontrar um vírus. Para fazer isso, marque a caixa de verificação **Exibir mensagem personalizada** em seguida, digite a mensagem que aparecerá na caixa de texto mostrada — pode ser digitada uma mensagem com 225 caracteres, no máximo. Depois, marque a caixa de verificação **Soar alerta audível**.

5. Clique na guia Relatório para escolher as opções do VShield adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do Filtro de Internet, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Relatório

O módulo Filtro de Internet do VShield registra quantos objetos Java e ActiveX foram examinados e quantos tiverem o acesso ao seu computador bloqueado, em um arquivo de registro chamado WEBFLTR.TXT. Esse mesmo arquivo registra o número de sites da Internet que você visitou enquanto o VShield estava ativo e quantos sites perigosos o programa impediu que o seu navegador visitasse.

O VShield poderá gravar o registro nesse arquivo ou usar um arquivo de texto criado com qualquer editor de texto. Esse arquivo de registro pode ser aberto e impresso para revisão posterior em qualquer editor de texto. Use a página de propriedades Relatório para especificar um arquivo que sirva como registro do Filtro de Internet do VShield e para determinar seu limite de tamanho.

Para configurar o VShield a fim de registrar suas ações em um arquivo de registro, siga estas etapas:

1. Clique na guia Relatório, no módulo Filtro de Internet para exibir a página de propriedades correta (Figura 4-34).
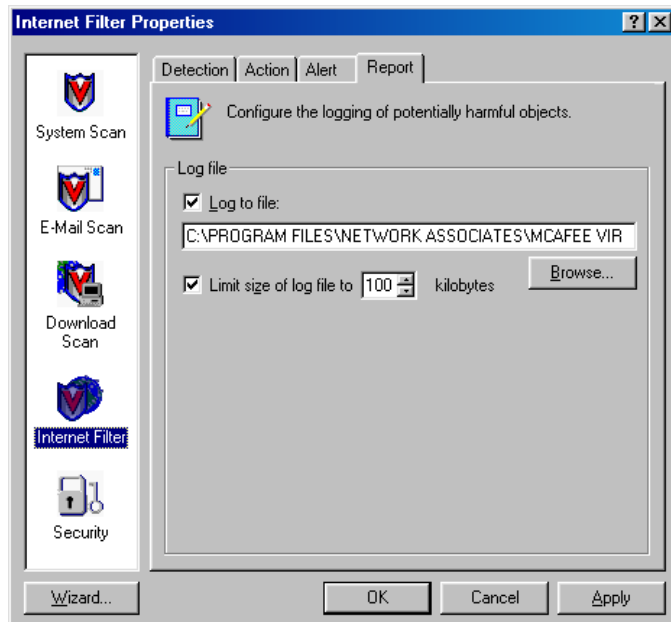
Figura 4-34. Caixa de diálogo Propriedades do Filtro de Internet – página Relatório

2. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, o VShield grava as informações de registro no arquivo WEBFLTR.TXT, no diretório de programa do VirusScan. Você pode digitar um nome e um caminho diferentes na caixa de texto mostrada, ou clicar em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

3. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o VShield limita o tamanho de arquivo em 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, o VShield apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

4. Clique em uma guia diferente para alterar as configurações do Filtro de Internet ou clique em um dos ícones na lateral da caixa de diálogo Propriedades do Filtro de Internet para escolher opções para outro módulo.

   Para salvar as alterações no módulo Filtro de Internet sem fechar a caixa de diálogo, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

   NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Configurando o módulo Segurança

Para manter as suas configurações do módulo Segurança a salvo de alterações não autorizadas, você pode proteger algumas ou todas as páginas de propriedades do módulo com uma senha. Se você for um administrador de sistemas, poderá usar esse recurso junto com a funcionalidade do VShield de salvar as configurações em um arquivo .VSH para replicar as suas opções de configuração em todos os computadores clientes na rede. Se o VShield não puder ser desativado (veja Etapa 4 na página 97 para obter mais detalhes), proteja a configuração com uma senha; você pode implantar uma política de segurança antivírus rigorosa para todos os usuários de rede, com facilidade e eficiência.

Use o módulo Segurança para atribuir um senha e escolher quais páginas serão protegidas.

Ativando a proteção por senha

Como padrão, o VShield não ativa o módulo Segurança, por que precisa saber qual a senha atribuída às configurações.

Para ativar e configurar a proteção por senha do VShield, siga estas etapas:

1. Marque a caixa de verificação **Ativar proteção por senha**.

   As opções restantes na página de propriedades são ativadas (Figura 4-35).
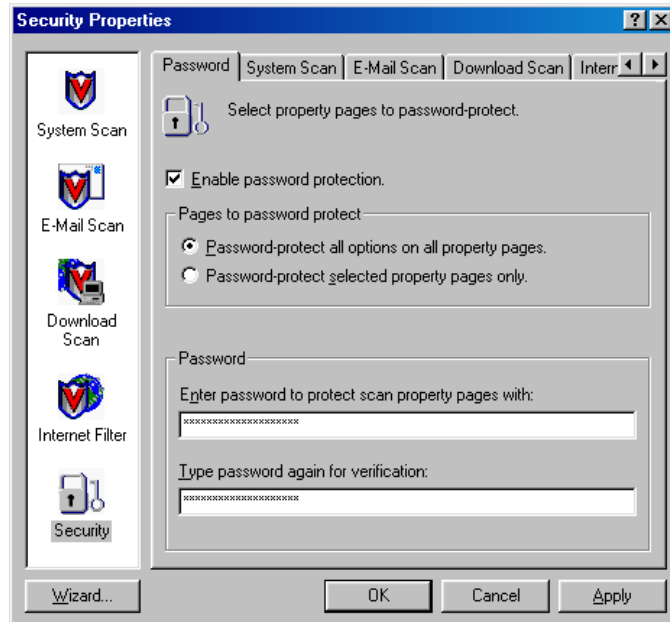
Figura 4-35. Caixa de diálogo Propriedades da Segurança – página Senha

2. Decida se você deseja proteger as páginas de propriedades de todos os módulos do VShield ou apenas páginas individuais. Estas são as opções:

   - **Proteger por senha as opções de todas as páginas de propriedades.** Selecione esse botão para bloquear tudo de uma só vez.

   - **Proteger por senha somente as páginas de propriedades selecionadas.** Selecione este botão para escolher quais páginas de propriedades em módulos individuais serão bloqueadas. As outras guias na caixa de diálogo Propriedades da Segurança permitem designar páginas individuais.

3. Digite uma senha que será usada para bloquear as suas configurações. Digite qualquer combinação de 20 caracteres, no máximo, na caixa de texto acima da área **Senha**, em seguida, repita exatamente a mesma combinação na caixa de texto de baixo para confirmar a senha.

   IMPORTANTE: A proteção por senha do VShield é diferente daquela atribuída no VirusScan. A escolha de uma senha para um componente não significa que será designada também para outros componentes — as senhas devem ser escolhidas para cada um deles separadamente.

4. Clique em qualquer uma das outras guias do módulo Segurança para proteger páginas de propriedades individuais. Para salvar a senha sem fechar a caixa de diálogo Propriedades da Segurança, clique em **Aplicar**. Se você preferir proteger as páginas de propriedades em todos os módulos e, depois, fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas alterações, clique em **Cancelar**.

   NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Após proteger as suas configurações com uma senha, o VShield lhe pedirá para digitá-la sempre que abrir a caixa de diálogo Propriedades do VShield (Figura 4-36).
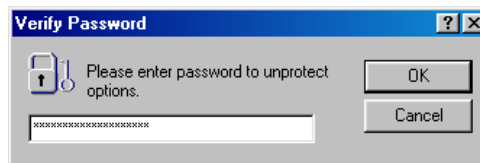
Figura 4-36. Caixa de diálogo Verificar senha

Digite a senha escolhida na caixa de texto mostrada, em seguida, clique em **OK** para ter acesso à caixa de diálogo Propriedades do VShield.

Protegendo páginas de propriedades individuais

Se você escolher **Proteger por senha somente as páginas de propriedades selecionadas** na página Senha do módulo de Segurança, poderá escolher quais opções de configuração deseja bloquear.

Siga estas etapas:

1. Clique na guia do *módulo* cujas configurações serão protegidas. Se você não vir a guia que procura, clique em ◄ ou ► para visualizá-la. Uma página típica aparece na Figura 4-37.
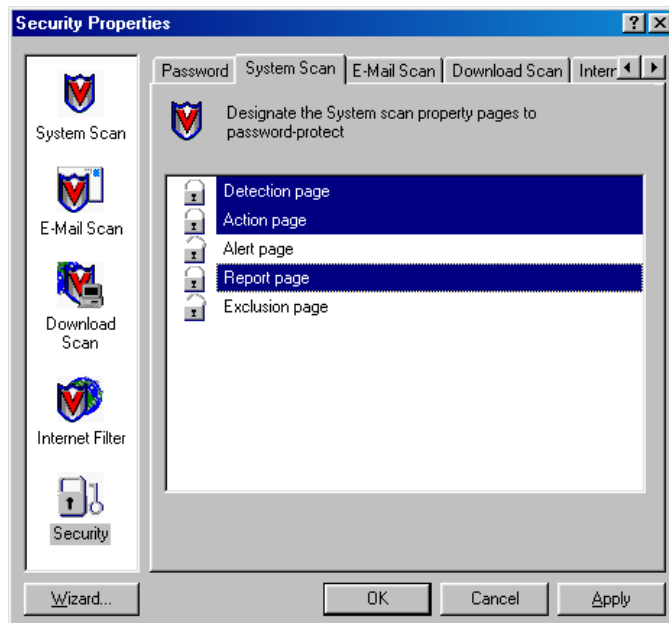
Figura 4-37. Opções de segurança da Varredura do Sistema

2. Selecione as configurações que você deseja proteger na lista mostrada.

   Você pode proteger algumas ou todas as páginas de propriedades de um módulo. As páginas de propriedades protegidas exibem um ícone de um cadeado fechado na lista de segurança mostrada na Figura 4-37. Para remover a proteção de uma página de propriedades, clique no cadeado fechado para abri-lo.

3. Selecione quantas páginas de propriedades você quiser proteger em cada módulo.

4. Para salvar a senha sem fechar a caixa de diálogo Propriedades da Segurança, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas alterações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Usando o menu de atalho do VShield

O VShield agrupa diversos entre os seus comandos comuns em um menu de atalho, associado ao seu ícone na barra de sistema . Clique duas vezes nesse ícone para exibir a caixa de diálogo Status do VShield. Clique no ícone com o botão direito do mouse para exibir esses comandos.

- **Status.** Escolha esta opção para abrir a caixa de diálogo Status do VShield.
- **Propriedades.** Aponte para esta opção, em seguida, escolha um dos módulos do VShield na lista, para abrir a caixa de diálogo Propriedades do VShield na página de propriedades para esse módulo.
- **Ativar.** Aponte para esta opção, em seguida, escolha um dos módulos do VShield na lista para ativar ou desativá-lo. Os módulos exibidos no menu com uma marca de verificação estão ativados, caso contrário, estão desativados.
- **Sobre.** Escolha esta opção para exibir o número da versão e o número de série do VShield, o número da versão e a data de criação dos arquivos .DAT que estão em uso atualmente, e um aviso de copyright da Network Associates.
- **Sair.** Escolha esta opção a fim de parar a operação de varredura de todos os módulos do VShield e descarregá-lo da memória.

Desativando ou parando o VShield

Uma vez iniciado, o VShield exibe um ícone na barra de sistema do Windows.A *desativação* do VShield o mantém em execução na memória, mas o impede de realizar funções de varredura. Quando são desativados todos os seus módulos, o VShield deixa um ícone “cancelado” na barra de sistema do Windows que você poderá usar para reativá-lo.

Quando é *parado* o VShield é removido da memória inteiramente — o seu ícone na barra de sistema do Windows também desaparecerá. Para reativá-lo a partir do mesmo ponto, você deve abrir a caixa de diálogo Propriedades do VShield e ativar de novo cada módulo individualmente (veja "Configurando as propriedades do VShield" na página 91 para obter mais detalhes) ou reinicie-o a partir do Programador de Tarefas do VirusScan.

O VShield pode ser desativado ou parado de um dos quatro modos seguintes:

- **No menu de atalho do VShield.** Clique no ícone do VShield na barra de sistema do Windows com o botão direito do mouse para exibir o menu de atalho, em seguida, escolha **Sair**.

  O VShield pára imediatamente, descarrega-se da memória e remove o seu ícone da barra de sistema do Windows.

  Para desativar módulos individuais do VShield, clique com o botão direito no ícone do VShield, aponte para **Ativar**, em seguida, escolha cada módulo individualmente. Os módulos que apresentarem uma marca de verificação ao lado estarão ativados, caso contrário estarão desativados.

  NOTA: Veja "Usando o menu de atalho do VShield" na página 147 para aprender mais sobre outras opções de menu.

- **Na caixa de diálogo Status do VShield.** Clique duas vezes no ícone do VShield na barra de sistema do Windows para exibir a caixa de diálogo Status do VShield (Figura 4-38).
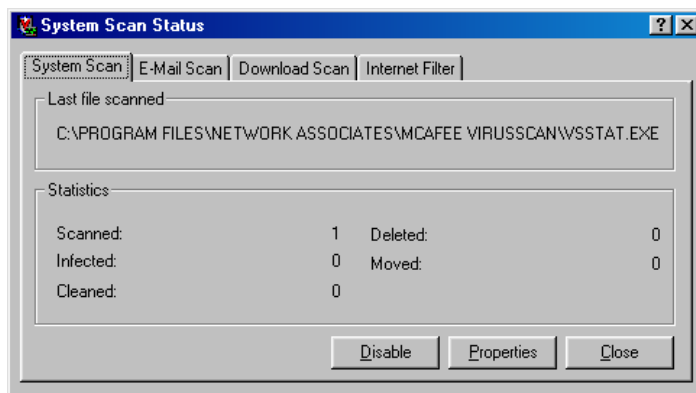
Figura 4-38. Caixa de diálogo Status

Para cada módulo que você quiser desativar, clique na guia correspondente, em seguida clique em **Desativar**. O VShield desativará esse módulo imediatamente. Depois que todos os seus módulos são desativados, o VShield exibirá na barra de sistema do Windows. Para reativar cada módulo, abra a caixa de diálogo Status, em seguida, clique em **Ativar** em cada página de propriedades.

- **Na caixa de diálogo Propriedades do VShield.** Clique no ícone do VShield na barra de sistema do Windows com o botão direito do mouse, aponte para **Propriedades**, em seguida escolha **Varredura do Sistema** no menu de atalho que aparece, para exibir a caixa de diálogo Propriedades do VShield (Figura 4-39).
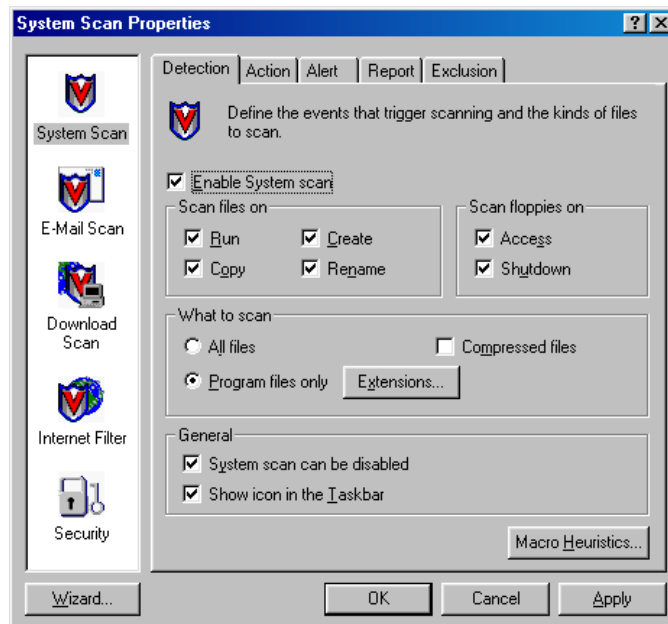
Figura 4-39. Caixa de diálogo Propriedades do VShield

Para cada módulo que você quiser desativar, clique na guia correspondente no lado esquerdo da caixa de diálogo, em seguida clique na guia Detecção. Depois, desmarque a caixa de seleção **Ativar**, na parte de cima de cada página. Em seguida, o VShield desativará esse módulo. Quando todos os módulos forem desativados, o VShield exibirá na barra de sistema do Windows, a menos que você tenha cancelado a verificação de **Mostrar ícone na barra de tarefas**.

Para reativar cada módulo, abra a caixa de diálogo Propriedades do VShield, em seguida marque a caixa de seleção **Ativar** na página Detecção de cada módulo.

- **No Programador de Tarefas do VirusScan.** Clique em **Iniciar** na barra de tarefas do Windows, aponte para **Programas**, em seguida para **McAfee VirusScan**. Depois, escolha **Programador de Tarefas do McAfee VirusScan** para abrir a janela do Programador de Tarefas (Figura 4-40).
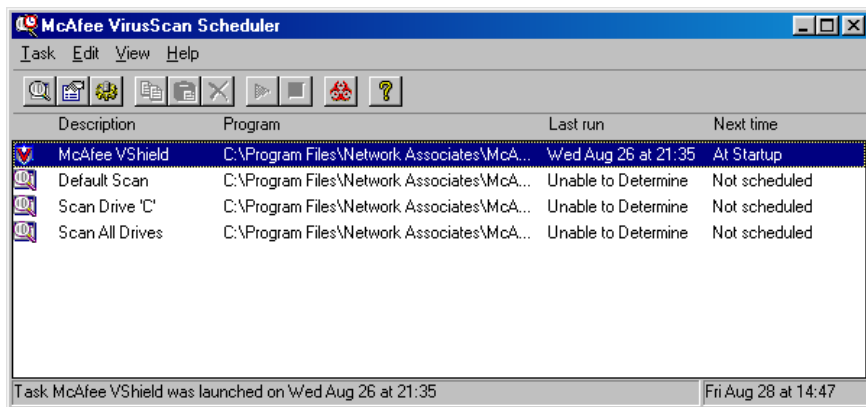
Figura 4-40. Janela do Programador de Tarefas do VirusScan

Selecione **McAfee VShield** na lista de tarefas, em seguida, escolha **Desativar** no menu **Tarefa**. O VShield desativará todos os seus módulos e exibirá na barra de sistema do Windows. Para reiniciar o VShield, selecione a tarefa VShield, em seguida, escolha **Ativar** no menu **Tarefa**.

Se você quiser parar o VShield completamente selecione **McAfee VShield** na lista de tarefas, em seguida clique em na barra de ferramentas do Programador de Tarefas. O VShield pára imediatamente, descarrega-se da memória e remove o seu ícone da barra de sistema do Windows. Para reativá-lo, selecione a tarefa VShield, em seguida, clique em .

Controlando informações de status do VShield

Quando estiver ativado e configurado, o VShield irá operar continuamente em segundo plano, observando e em seguida examinando o correio eletrônico recebido, os arquivos que você executa ou obtém por download, ou os objetos Java e ActiveX encontrados.

Para ver um resumo do seu andamento:

1. Abra uma caixa de diálogo Status do VShield. Isso pode ser feito de duas maneiras:

   - Clique duas vezes no ícone na barra de sistema do VShield ; para abrir a caixa de diálogo Status mostrada na Figura 4-38 na página 148; ou

   - Abra o Programador de Tarefas do VirusScan, selecione a tarefa do VShield na lista de tarefas, em seguida clique em na barra de ferramentas do Programador de Tarefas para exibir a caixa de diálogo Propriedades da Tarefa mostrada em Figura 4-41.
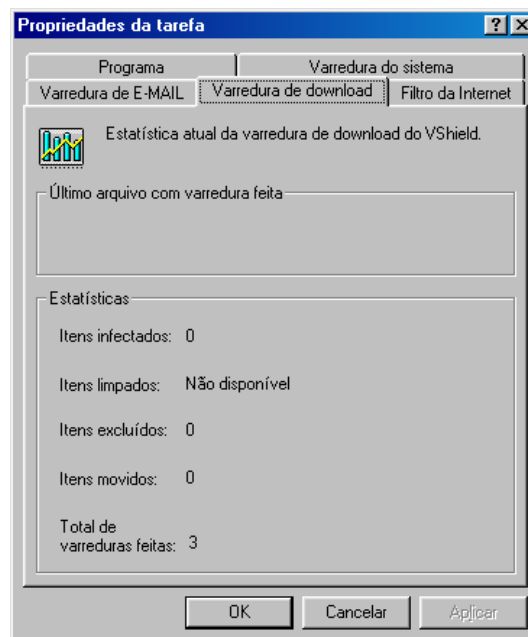
Figura 4-41. Caixa de diálogo Propriedades de Tarefa do VShield

2. Clique na guia que corresponde ao componente de programa que você deseja ativar ou desativar, ou para verificar o andamento.

   Para o módulo Varredura do Sistema, o VShield relata o número de arquivos examinados, o número de arquivos infectados encontrados e o número de arquivos que foram limpos, movidos ou excluídos. Para os módulos Varredura de Correio Eletrônico e Varredura de Download, o programa relata o número de arquivos examinados, o número de infecções encontradas e o número de arquivos movidos ou excluídos. O VShield relata o número de itens de miniaplicativos Java e ActiveX, ou de sites da Internet examinados e quantos foram “banidos”, mantidos fora de seu alcance.

   Se o recurso de relatório estiver ativado, o VShield também incluirá as mesmas informações no arquivo de registro para cada módulo.

Se você escolheu o primeiro método descrito em Etapa 1 na página 151 para abrir uma caixa de diálogo Status, poderá também ativar ou desativar o VShield, ou abrir a caixa de diálogo Propriedades do VShield. Você pode:

- Clicar na guia que corresponde ao componente de programa que será ativado ou desativado, depois em **Ativar** para iniciá-lo. Clicar em **Desativar** para desativá-lo. Veja “Desativando ou parando o VShield” na página 147 para saber mais sobre outros modos de ativar e desativar o VShield.
- Clicar em **Propriedades** para abrir a caixa de diálogo Propriedades do VShield, na qual você define as opções que indicam ao VShield como executar cada tipo de varredura. Veja “Configurando as propriedades do VShield” na página 91 para saber como escolher as opções de configuração na caixa de diálogo Propriedades do VShield.

Usando o McAfee VirusScan 5

O que é o VirusScan?

O nome VirusScan aplica-se ao conjunto de componentes de programa antivírus para área de trabalho descrito neste *Guia do Usuário* e a um componente em particular desse conjunto: SCAN32.EXE ou a varredura "por solicitação" do VirusScan. "Por solicitação" significa que você, enquanto usuário, controla quando o VirusScan inicia e termina uma operação de varredura, quais os alvos examinados, o que faz quando encontra um vírus ou qualquer outro aspecto do funcionamento do programa. Por outro lado, os outros componentes do VirusScan operam automaticamente ou segundo um planejamento que você define. O VirusScan consistia originalmente apenas de uma varredura por solicitação — os recursos que foram sendo integrados ao programa agora fornecem um conjunto de funções antivírus que oferecem máxima proteção contra infecções por vírus e ataques de software destrutivo.

O componente por solicitação do VirusScan opera de dois modos: a interface do VirusScan "Clássico" faz com que você o instale e comece a trabalhar rapidamente, com um mínimo de opções de configuração, mas com toda a potência do mecanismo de varredura antivírus do VirusScan; o modo Avançado do VirusScan torna as opções de configuração do programa flexíveis, incluindo a possibilidade de executar mais de uma operação de varredura simultaneamente.

Este capítulo descreve como usar o VirusScan nos modos Clássico e Avançado.

Por que executar operações de varredura por solicitação?

Como o componente VShield fornece proteção de varredura em segundo plano, a utilização do VirusScan para examinar o seu sistema pode parecer redundante. Mas as boas medidas de segurança antivírus incorporam varreduras do sistema regulares e completas porque:

- **A varredura em segundo plano verifica os arquivos que estão em execução.** O VShield procura código de vírus enquanto os arquivos executáveis são executados ou quando você lê um disquete, mas o VirusScan pode examinar assinaturas de códigos em arquivos armazenados no seu disco rígido. Se um arquivo infectado for executado raramente, o VShield pode não detectar o vírus até que ele distribua sua carga explosiva. Contudo, o VirusScan pode detectar um vírus enquanto estiver aguardando oportunidade para ser executado.

- **Os vírus são furtivos.** Ao deixar acidentalmente um disquete na unidade, quando você iniciar o computador o vírus poderá ser carregado na memória, antes que o VShield inicie, particularmente se não estiver configurado para examinar os disquetes. Uma vez na memória, um vírus pode infectar quase todos os programas, incluindo o VShield.

- **A varredura com o VShield gasta tempo e recursos.** A varredura em busca de vírus quando você executa, copia ou salva arquivos pode retardar ligeiramente os tempos de inicialização de software e outras tarefas. Dependendo das suas condições, esse tempo poderia ser utilizado em trabalhos importantes. Embora o impacto seja muito pequeno, você pode ser tentado a desativar o VShield, se precisar de toda a potência para as tarefas mais exigentes. Nesse caso, a realização de operações de varredura regulares, durante o tempo ocioso, pode proteger o seu sistema contra infecção sem comprometer o desempenho.

- **Boa segurança é uma segurança redundante.** Num mundo ligado em rede, centralizado na Web, no qual a maioria dos usuários de computadores operam atualmente, o download de vírus de uma origem que talvez você nem se lembre de ter visitado, é instantâneo. Se um conflito de software tiver desativado a varredura em segundo plano naquele momento, ou se a varredura em segundo plano não tiver sido configurada para observar um ponto de entrada vulnerável, pode ocorrer infecção por vírus. As operações de varredura regulares podem, com freqüência, detectar infecções antes que se espalhem ou causem danos.

O VirusScan Classic contém uma única operação de varredura padrão pré-configurada e pronta para ser executada. Você pode iniciar essa operação de varredura para procurar vírus na unidade C: imediatamente, ou configurar e executar as suas operações de varredura para atender às suas necessidades. O VirusScan Advanced também contém uma única operação de varredura pré-configurada, que examina todos os seus discos rígidos locais.

Iniciando o VirusScan

Para iniciar o VirusScan, escolha um dos seguintes procedimentos

- Clique em **Iniciar** na barra de tarefas do Windows, aponte para **Programas**, em seguida para **McAfee VirusScan**. Depois, escolha **McAfee VirusScan** na lista mostrada; ou

- Clique em **Iniciar**, em seguida, escolha **Executar** no menu mostrado. Digite SCAN32.EXE na caixa de diálogo Executar, em seguida, clique em **OK**.

Ambos os métodos abrem a janela do VirusScan Classic (Figura 5-1).
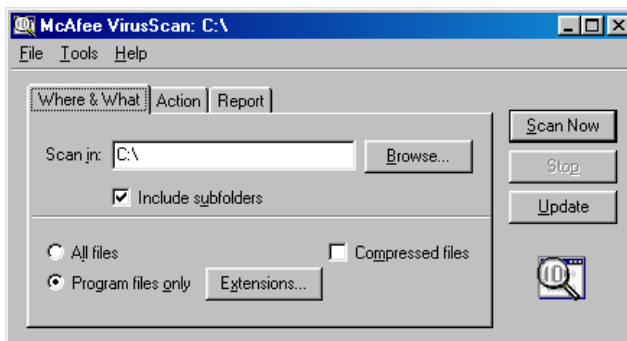
Figura 5-1. Janela do VirusScan Classic

Clique em **Examinar agora** no lado direito da janela para iniciar a tarefa de varredura imediatamente, ou configurar uma tarefa de varredura que atenda às suas necessidades, clicando nas guias, na parte superior da janela, e escolhendo opções em cada página de propriedades.

Usando os menus do VirusScan

Os menus que estão na parte superior da janela do VirusScan permitem alterar alguns aspectos da operação do programa. Você pode:

- **Salvar ou restaurar as configurações padrão.** Como padrão, o VirusScan Classic procura vírus nos arquivos mais suscetíveis a infecção por vírus. Ele examinará as área do sistema e da memória, a unidade C: e todas as suas subpastas, em seguida emitirá um alerta sonoro e solicitará que você defina uma ação quando o programa encontrar um vírus. O programa também irá registrar suas ações e resumir as configurações atuais em um arquivo de registro que você pode rever posteriormente.

  Se você alterar essas definições e quiser salvá-las para que se tornem as novas configurações padrão, escolha **Salvar como Padrão** no menu **Arquivo** ou clique no botão **Nova Varredura**, à direita na janela do VirusScan Classic. O VirusScan lhe pedirá para confirmar se deseja substituir o arquivo que registra as configurações padrão. Clique em **Sobrepor** ou **OK** para continuar. O VirusScan gravará as suas opções para usá-las em cada operação de varredura realizada após esses procedimentos.

NOTA: Se você alterar as definições padrão mas decidir retornar aos parâmetros originais do VirusScan, utilize o Windows Explorer para localizar e excluir o arquivo DEFAULT.VSC no diretório de programas do VirusScan. Ao iniciar posteriormente o VirusScan, o programa irá restaurar e salvar as suas configurações padrão em um novo arquivo DEFAULT.VSC. Para conhecer o formato de arquivo .VSC, veja Apêndice C, “Compreendendo o formato de arquivo .VSC.”

- **Salvar novas configurações.** Se você precisar de configurações diferentes do VirusScan para executar várias operações de varredura, ou se quiser executar uma varredura com as mesmas definições em mais de um computador, poderá salvar as suas opções de configuração como um arquivo .VSC com seu próprio nome. Este é um arquivo de texto que registra as opções de configuração do VirusScan, semelhante aos arquivos .INI do Windows que registram as opções de inicialização do programa.

  Para salvar as suas configurações, primeiro configure o VirusScan com as opções desejadas, em seguida, escolha **Salvar configurações** no menu **Arquivo**. Digite um nome descritivo na caixa de diálogo Salvar como, escolha uma localização para o arquivo no disco rígido, em seguida, clique em **Salvar**. Depois, você pode copiar esse arquivo para qualquer outro computador que vá usar essas configurações. Veja “Configurando o VirusScan Classic” na página 158 ou “Configurando o VirusScan Advanced” na página 164 para obter mais detalhes.

  Para executar o VirusScan com essas configurações, basta localizar e clicar duas vezes no arquivo .VSC salvado. Isto iniciará o VirusScan com as configurações carregadas.

- **Abra o registro de atividades do VirusScan.** Escolha **Exibir registro de atividades** no menu **Arquivo**, para abrir o arquivo de registro que o VirusScan usa para registrar suas ações e configurações.

  O arquivo de registro será aberto em uma janela do Bloco de Notas (Figura 5-2 na página 157). Você pode imprimir, editar, copiar ou tratá-lo como qualquer outro arquivo de texto comum. Para saber mais sobre quais informações são incluídas no arquivo de registro, veja “Escolhendo opções de Relatório” na página 175.

Figura 5-2. Registro de Atividades do VirusScan

- **Sair do VirusScan.** Escolha **Fechar** no menu **Arquivo** para sair do VirusScan. Quando você sai do VirusScan todas as atividades são interrompidas, mas isso *não* afeta as operações em segundo plano contínuas do VShield. A menos que você as salve, as opções de configuração escolhidas também desaparecerão ao sair do VirusScan.

- **Alterar modos do VirusScan.** Escolha **Avançado** no menu **Ferramentas** para alternar do VirusScan Classic para o VirusScan Advanced. Para alternar do VirusScan Advanced para o VirusScan Classic, escolha **Clássico** no menu **Ferramentas**.

- **Ativando a proteção por senha.** Escolha **Proteger por Senha** no menu **Ferramentas** para abrir a caixa de diálogo na qual é possível escolher as opções de configuração do VirusScan que devem ser bloqueadas para impedir alterações não autorizadas. Veja “Ativando a proteção por senha” na página 181 para obter mais detalhes.

- **Iniciar o Programador de Tarefas do VirusScan.** Escolha **Programador de Tarefas** no menu **Ferramentas** para abrir o Programador de Tarefas do VirusScan, um utilitário que permite configurar e executar operações de varredura sem acompanhamento. Para saber como usar o Programador de Tarefas, veja “Planejando tarefas de varredura” na página 183.

- **Abrir o arquivo da ajuda online.** Escolha **Tópicos da Ajuda** no menu **Ajuda** para ver uma lista de tópicos da ajuda do VirusScan. Para ver uma descrição contextual dos botões, listas e outros itens na janela do VirusScan, escolha **O que é isto?** no menu **Ajuda**, em seguida clique em um item com botão esquerdo do mouse depois que o cursor do mouse tomar a forma de . Você pode ver estes mesmos tópicos da ajuda se clicar com o botão direito do mouse em um elemento na janela do VirusScan, em seguida escolher **O que é isto?** no menu mostrado.

Configurando o VirusScan Classic

Para executar uma operação de varredura, o VirusScan precisa saber o que vai examinar, o que irá fazer ao encontrar um vírus e como deverá informar-lhe quando isto acontecer. Você também pode instruir ao VirusScan para que registre as suas ações. Uma série de páginas de propriedades controla as opções para cada tarefa — clique em cada guia na janela do VirusScan Classic para configurá-lo para a sua tarefa.

Escolhendo as opções Onde e o quê

O VirusScan assume inicialmente que você deseja examinar a unidade C: e todas as suas subpastas, e restringir os arquivos apenas àqueles suscetíveis a infecção por vírus (Figura 5-3).
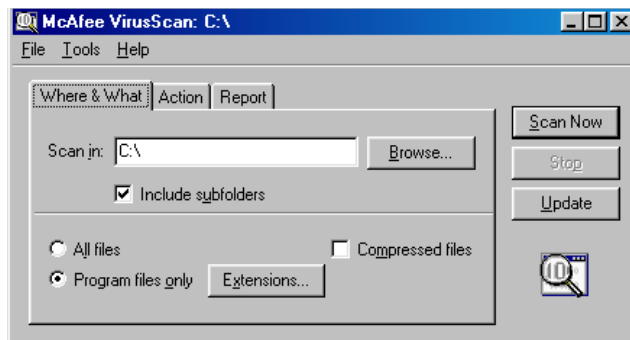
Figura 5-3. Janela do VirusScan Classic – página Onde e o quê

Para modificar essas opções, siga estas etapas:

1. Escolha um volume ou pasta no seu sistema ou na rede que o VirusScan examinará em busca de vírus.

   Você pode digitar um destino para o volume ou a pasta de destino na caixa de texto **Examinar em** ou clique em **Procurar** para abrir a caixa de diálogo Procurar pasta (Figura 5-4 na página 159).

Figura 5-4. Caixa de diálogo Procurar pasta

Clique em ⊞ para expandir a listagem de um item mostrado na caixa de diálogo. Clique em ⊟ para reduzir um item. Você pode selecionar discos rígidos, pastas ou arquivos como alvos das varreduras, estejam eles residindo no seu sistema ou em outros computadores da rede. Não é permitido selecionar Meu Computador, Área da Rede ou diversos volumes como destinos de varredura no VirusScan Classic — para escolhê-los, é necessário alternar para o VirusScan Advanced.

Após selecionar o seu destino de varredura, clique em **OK** para retornar à janela do VirusScan Classic.

2. Marque a caixa de verificação **Incluir subpastas** para que o VirusScan procure vírus nas pastas contidas no destino de varredura.

3. Especificar quais tipos de arquivos o VirusScan deverá examinar. Você pode

   - **Examinar arquivos compactados.** Marque a caixa de verificação **Arquivos compactados** para que o VirusScan procure vírus em arquivos compactados nos seguintes formatos: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Embora proporcione melhor proteção, a varredura de arquivos compactados pode tornar mais lenta uma operação de varredura.

- **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Contudo, você pode reduzir seguramente a abrangência das operações de varredura a esses arquivos mais suscetíveis a infecções por vírus, a fim de acelerá-las. Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou designar as extensões de nomes de arquivos que o VirusScan examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (Figura 5-5).

Figura 5-5. Caixa de diálogo Extensões de arquivo de programa

Como padrão, o VirusScan procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .MD?, .VXD, .SYS, .BIN, .RTF, .OBD e .DLL. Os arquivos com as extensões .DO?, .XL?, .RTF, .MD? e .OBD pertencem ao Microsoft Office, sendo que todos podem ser infectados por vírus de macro. O ? é um coringa que possibilita ao VirusScan examinar arquivos de modelos e de documentos.

– Para adicionar uma extensão na lista, clique em **Adicionar**, em seguida, digite as extensões que o VirusScan deverá examinar na caixa de diálogo mostrada.

– Para remover uma extensão da lista, selecione-a e clique em **Remover**.

– Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

Para que o VirusScan examine todos os arquivos do seu sistema, com qualquer extensão, selecione o botão **Todos os arquivos**. Embora este procedimento ofereça mais proteção, tornará as operações de varredura consideravelmente mais lentas.

4. Clique na guia Ação para escolher opções do VirusScan adicionais.

   Para iniciar uma operação de varredura imediatamente apenas com as opções escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar como padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Escolhendo opções de Ação

Quando o VirusScan detecta um vírus, poderá lhe perguntar o que deve fazer com o arquivo infectado, ou atuar automaticamente realizando uma ação predeterminada. Use a página de propriedades Ação para especificar quais opções de ação o VirusScan deve lhe propor ao encontrar um vírus ou quais as ações que o programa deve realizar automaticamente.

Siga estas etapas:

1. Clique na guia Ação, na janela do VirusScan Classic, para exibir a página de propriedades correta (Figura 5-6).

Figura 5-6. Janela do VirusScan Classic – página Ação

2. Escolha uma ação na lista **Quando um vírus for encontrado**. A área imediatamente abaixo da lista será alterada para mostrar as opções adicionais para cada ação. Estas são as opções:

   - **Solicitar ação ao usuário.** Escolha esta ação se você pretende estar usando o seu computador quando o VirusScan examinar o disco — o programa exibirá uma mensagem de alerta ao encontrar um vírus e oferecerá uma ampla gama de opções de ação disponíveis.

- **Mover arquivos infectados automaticamente**. Escolha esta opção para que o VirusScan mova os arquivos infectados para um diretório de quarentena logo após encontrá-los. Como padrão, o VirusScan move esses arquivos para uma pasta chamada INFECTADO, criada no nível raiz da unidade na qual o vírus foi encontrado. Por exemplo, se o VirusScan encontrar um arquivo infectado em T:\MEUS DOCUMENTOS e for especificada a pasta INFECTADO como o diretório de quarentena, o programa copiará o arquivo para T:\INFECTADO.

  Você pode digitar um nome na caixa de texto mostrada, ou clicar em **Procurar** para localizar uma pasta adequada no disco rígido.

- **Limpar arquivos infectados automaticamente.** Escolha esta opção para que o VirusScan remova o código do vírus do arquivo infectado assim que for encontrado. Se o VirusScan não puder remover o vírus, a ocorrência será incluída no arquivo de registro. Veja o “Escolhendo opções de Relatório” na página 175 para obter mais detalhes.

- **Excluir arquivos infectados automaticamente.** Use esta opção para que o VirusScan exclua imediatamente os arquivos infectados encontrados. Certifique-se de ter ativado o recurso de relatório para que você tenha um registro de quais arquivos o programa excluiu. Será necessário restaurar os anexos excluídos a partir de cópias de backup. Se o VirusScan não puder excluir um arquivo infectado a ocorrência será incluída no arquivo de registro.

- **Continuar a varredura.** Use esta opção se você pretende afastar-se do computador enquanto o VirusScan examina a ocorrência de vírus. Se as opções de relatório também estiverem ativadas, o programa (veja “Escolhendo opções de Relatório” na página 175 para obter mais detalhes), registrará os nomes dos vírus e os nomes de arquivos infectados para que você possa excluí-los na próxima oportunidade.

3. Clique na guia Relatório para escolher as opções do VirusScan adicionais.

   Para iniciar uma operação de varredura imediatamente apenas com as operações escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar com padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Escolhendo opções de Relatório

Como padrão, o VirusScan emite um sinal sonoro para alertá-lo quando o programa encontra um vírus. Você pode usar a página Relatório para ativar ou desativar esse alerta, ou para adicionar uma mensagem de alerta na caixa de diálogo Vírus encontrado, que aparece quando o VirusScan encontra um arquivo infectado. Essa mensagem de alerta pode conter qualquer informação, de uma simples advertência a instruções sobre o modo que relata o incidente ao administrador de rede.

Esta mesma página determina o tamanho e a localização do arquivo de registro do VirusScan. Como padrão, o programa faz uma lista das configurações atuais e resume todas as ações efetuadas durante as operações de varredura em um arquivo de registro chamado VSCLOG.TXT. O VirusScan pode gravar esse registro em um arquivo ou você poderá usar qualquer editor de texto para criar um arquivo de texto para ser usado pelo VirusScan. Você pode, em seguida, abrir e imprimir o arquivo de registro para utilizá-lo posteriormente no VirusScan ou em um editor de texto.

Para escolher as opções de alerta e de registro do VirusScan siga estas etapas:

1. Clique na guia Relatório, na janela do VirusScan Classic para exibir a página de propriedades correta (Figura 5-7).
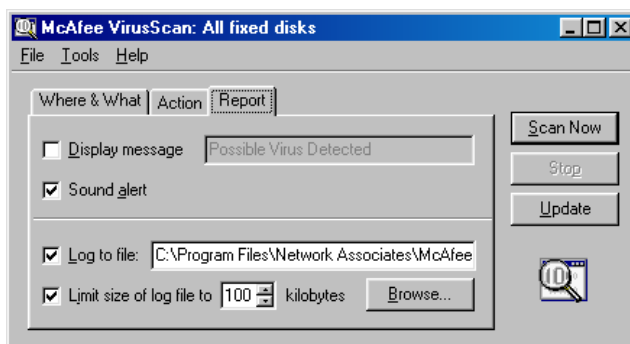
Figura 5-7. Janela do VirusScan Classic – página Relatório

2. Escolha os tipos de métodos de alerta que VirusScan deve usar quando encontrar vírus. O VirusScan pode:

   - **Exibir mensagem personalizada.** Marque a caixa de verificação **Exibir mensagem**, em seguida digite a mensagem que deverá ser exibida na caixa de texto mostrada. A mensagem pode conter 225 caracteres no máximo.

> **NOTA:** Para que o VirusScan exiba a sua mensagem, você deve ter selecionado **Solicitar ação ao usuário** como a sua opção de ação na página Ação (veja "Escolhendo opções de Ação" na página 171 para obter mais detalhes).

- **Sinal sonoro.** Marque a caixa de verificação **Soar alerta**.

3. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, o VirusScan grava as informações de registro no arquivo VSCLOG.TXT, no diretório de programa do VirusScan. Você pode digitar um nome e um caminho diferentes na caixa de texto mostrada, ou clicar em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

4. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o VShield limita o tamanho de arquivo para 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, o VShield apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

5. Clique em uma guia diferente para alterar as suas configurações do VirusScan.

   Para iniciar uma operação de varredura imediatamente apenas com as opções escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar como padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Configurando o VirusScan Advanced

O VirusScan Advanced oferece maior flexibilidade em suas opções de configuração do que o VirusScan Classic, incluindo a possibilidade de executar mais de uma operação de varredura simultaneamente, excluir itens de operações de varredura e ativar o recurso de detecção heurística do VirusScan.

Iniciando o VirusScan Advanced

Para iniciar o VirusScan Advanced, siga estas etapas:

1. Clique em **Iniciar** na barra de tarefas do Windows, aponte para **Programas**, em seguida para **McAfee VirusScan**. Em seguida, escolha **McAfee VirusScan** na lista mostrada.

   Esse procedimento abre a janela do VirusScan Classic (veja Figura 5-1 na página 155).

2. Escolha **Avançado** no menu **Ferramentas** na janela do VirusScan Classic para alternar para o modo Avançado do VirusScan.

Como no VirusScan Classic, uma série de páginas de propriedades controlam as opções para cada tarefa no VirusScan Advanced. Clique em cada guia na janela do VirusScan Advanced para configurar a sua tarefa no VirusScan. As próximas seções descrevem as opções disponíveis.

Escolhendo opções de Detecção

O VirusScan supõe inicialmente que você irá examinar todos os discos rígidos do seu computador, incluindo aqueles mapeados nas unidades de rede e restringir os arquivos examinados aos mais suscetíveis a infecções por vírus somente (Figura 5-8).
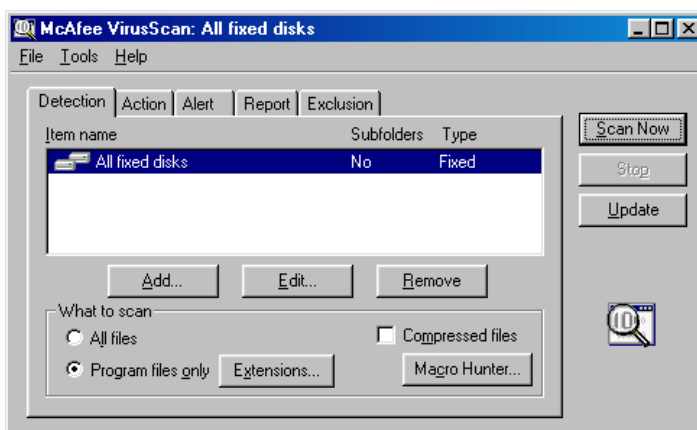
Figura 5-8. Janela do VirusScan Advanced – página Detecção

Para modificar estas opções e adicionar outras, siga estas etapas:

1. Escolha quais partes do sistema ou da rede o VirusScan examinará para procurar vírus. Você pode:

   - **Adicionar destinos de varredura.** Clique em **Adicionar** para abrir a caixa de diálogo Adicionar item de varredura (Figura 5-9).
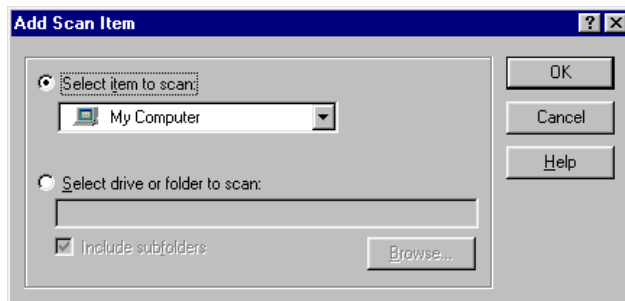
Figura 5-9. Caixa de diálogo Adicionar item de varredura

Para que o VirusScan examine o computador inteiro ou um subconjunto de unidades no sistema ou na rede, clique no botão **Selecionar item para varredura**, em seguida, escolha o destino da varredura na lista fornecida.

Estas são as opções:

– **Meu Computador.** Esta opção informa ao VirusScan para examinar todas as unidades fisicamente anexadas ao computador ou logicamente mapeadas através do Windows Explorer para uma letra de unidade no seu computador.

– **Toda a mídia removível.** Esta opção instrui o VirusScan a examinar apenas os discos de CD-ROM, discos ZIP da Iomega ou dispositivos de armazenamento semelhantes fisicamente anexados ao seu computador.

– **Todos os discos rígidos.** Esta opção informa ao VirusScan para examinar discos rígidos conectados fisicamente ao computador.

– **Todas as unidades de rede.** Esta opção informa ao VirusScan para examinar todas as unidades de disco logicamente mapeadas através do Windows Explorer para uma unidade no seu computador.

Para que o VirusScan examine um disco ou pasta específica no sistema, clique no botão **Selecionar unidade ou pasta para examinar**. Em seguida, digite a letra da unidade ou o caminho para a pasta a ser examinada, na caixa de texto mostrada, ou clique em **Procurar** para localizar o destino da varredura no computador. Marque a caixa de verificação **Incluir subpastas** para que o VirusScan também procure vírus em qualquer pasta contida no destino da varredura. Clique em **OK** fechar a caixa de diálogo.

- **Alterar destinos de varredura.** Selecione um dos destinos de varredura da lista, em seguida, clique em **Editar** para abrir a caixa de diálogo Editar item de varredura (Figura 5-10).
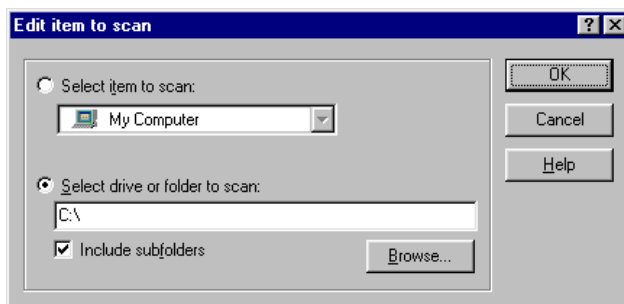
Figura 5-10. Caixa de diálogo Editar item para varredura

A caixa de diálogo aparece com o destino de varredura especificado. Escolha ou digite um novo destino de varredura, em seguida, clique em **OK** para fechar a caixa de diálogo.

- **Remover destinos de varredura.** Selecione um dos destinos de varredura na lista, em seguida, clique em **Remover** para excluí-lo.

2. Especificar quais tipos de arquivos o VirusScan deverá examinar. Você pode

- **Examinar arquivos compactados.** Marque a caixa de verificação **Arquivos compactados** para que o VirusScan procure vírus em arquivos compactados nos formatos: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Embora esse procedimento lhe ofereça melhor proteção, a varredura de arquivos compactados pode alongar mais uma operação de varredura.

- **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Contudo, você pode reduzir seguramente a abrangência das operações de varredura a esses arquivos mais suscetíveis a infecções por vírus, a fim de acelerá-las. Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou designar as extensões de nomes de arquivos que o VirusScan examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (Figura 5-11).
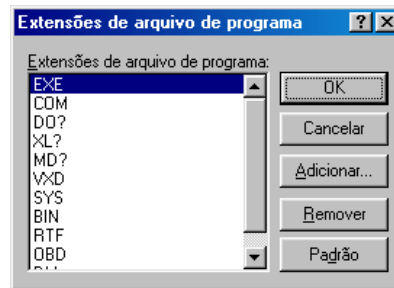
Figura 5-11. Caixa de diálogo Extensões de arquivo de programa

Como padrão, o VirusScan procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .MD?, .VXD, .SYS, .BIN, .RTF, .OBD e .DLL. Os arquivos com as extensões .DO?, .XL?, .RTF, .MD? e .OBD pertencem ao Microsoft Office, sendo que todos podem ser infectados por vírus de macro. O ? é um curinga que possibilita ao VirusScan examinar arquivos de modelos e de documentos.

– Para adicionar uma extensão na lista, clique em **Adicionar**, em seguida, digite as extensões que o VirusScan deverá examinar na caixa de diálogo mostrada.

– Para remover uma extensão da lista, selecione-a, em seguida clique em **Remover**.

– Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

Para que o VirusScan examine todos os arquivos do seu sistema, com qualquer extensão, selecione o botão **Todos os arquivos**. Embora este procedimento ofereça mais proteção, tornará as operações de varredura consideravelmente mais lentas.

- **Ativar a varredura heurística**. Clique em **Heurística** para abrir a caixa de diálogo Configurações da varredura heurística (Figura 5-12).

Figura 5-12. Caixa de diálogo Configurações da varredura heurística

A tecnologia da varredura heurística possibilita ao VirusScan reconhecer novos vírus de macros com base na sua semelhança com vírus similares que o programa já conhece. Para fazê-lo, o programa procura características “semelhantes a vírus” nos arquivos que você designou para serem examinados. A presença de um número suficiente desses elementos em um arquivo, leva o VirusScan a identificar o arquivo como potencialmente infectado com um novo vírus ou qualquer outro anteriormente não identificado.

Como o VirusScan procura simultaneamente pelas características do arquivo que excluem a possibilidade de infecção, ele raramente lhe dará uma falsa indicação sobre uma infecção por vírus. Contudo, a menos que você saiba que o arquivo *não* contém vírus, deverá tratar as infecções “em potencial” com o mesmo cuidado que as confirmadas.

Para ativar a varredura heurística, siga estas etapas

a. Marque a caixa de verificação **Ativar a varredura heurística**. As opções restantes na caixa de diálogo são ativadas.

b. Selecione os tipos de varredura heurística que o VirusScan deverá utilizar. Estas são as opções:

- **Ativar a varredura heurística de macro**. Escolha esta opção para que o VirusScan identifique todos os arquivos do Microsoft Word, Microsoft Excel e outros do Microsoft Office que tenham macros incorporadas, em seguida compare o código da macro com o banco de dados de assinaturas de vírus. O VirusScan verificará as correspondências exatas com o nome do vírus; as assinaturas de código semelhantes àquelas de vírus existentes fazem com que o programa lhe informe que encontrou um provável vírus de macro.

- **Ativar a varredura heurística de arquivos de programa.** Escolha esta opção para que o VirusScan localize vírus em arquivos de programa examinando as suas características e comparando-as a uma lista de especificações de vírus conhecidos. O programa identificará os arquivos com um número suficiente dessas características como vírus prováveis.

- **Ativar a varredura heurística de arquivos de programa e macros.** Escolha esta opção para que o VirusScan use ambos os tipos de varredura heurística. A Network Associates recomenda que você use essa opção para obter uma proteção completa antivírus.

c. Determinar como deseja tratar os arquivos de macros infectados. Selecione **Remover todas as macros ao limpar documentos infectados** para eliminar todos os códigos infectantes do documento e deixar apenas os dados. Para tentar eliminar apenas os códigos de vírus das macros de documentos, não marque essa caixa de verificação.

ATENÇÃO: Use esse recurso com cuidado: a remoção de todas as macros de um documento pode causar a perda de dados ou danificá-lo, tornando o documento inútil.

---

d. Clique em **OK** para salvar as suas configurações e retornar à janela do VirusScan Advanced.

3. Clique na guia Ação para escolher opções do VirusScan adicionais.

   Para iniciar uma operação de varredura imediatamente apenas com as opções escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar como padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Escolhendo opções de Ação

Quando o VirusScan detecta um vírus, poderá lhe perguntar o que deve fazer com o arquivo infectado, ou atuar automaticamente realizando uma ação predeterminada. Use a página de propriedades Ação para especificar quais opções de ação o VirusScan deve lhe propor ao encontrar um vírus ou quais as ações que o programa deve realizar automaticamente.

Siga estas etapas:

1. Clique na guia Ação na janela do VirusScan Advanced para exibir a página de propriedades correta (Figura 5-13).

Figura 5-13. VirusScan Advanced – página Ação

2. Escolha uma ação na lista **Quando um vírus for encontrado**. A área imediatamente abaixo da lista será alterada para mostrar as opções adicionais para cada ação. Estas são as opções:

- **Solicitar ação ao usuário.** Escolha esta ação se você pretende estar usando o seu computador quando o VirusScan examinar o disco — o programa exibirá uma mensagem de alerta ao encontrar um vírus e oferecerá uma ampla gama de opções de ação disponíveis:
  - **Limpar infecção.** Esta opção informa ao VirusScan para tentar remover o código de vírus do arquivo infectado.
  - **Excluir arquivo.** Esta opção informa ao VirusScan para excluir o arquivo infectado imediatamente.
  - **Excluir o item da varredura.** Esta opção informa ao VirusScan para ignorar o arquivo durante as próximas operações de varredura. Esta é a única opção que não é selecionada como padrão.
  - **Continuar a varredura.** Esta opção informa ao VirusScan para continuar a varredura, mas não atuar de qualquer outra maneira. Se as opções de relatório estiverem ativadas, o VirusScan incluirá a ocorrência no arquivo de registro.
  - **Parar a varredura.** Esta opção informa ao VirusScan que deve parar a operação de varredura imediatamente. Para continuar, você deve clicar em **Examinar agora** para reiniciar a operação.
  - **Mover arquivo.** Esta opção informa ao VirusScan para mover o arquivo infectado para um diretório de quarentena.
- **Mover arquivos infectados automaticamente**. Escolha esta opção para que o VirusScan mova os arquivos infectados para um diretório de quarentena logo após encontrá-los. Como padrão, o VirusScan move esses arquivos para uma pasta chamada INFECTADO, criada no nível raiz da unidade na qual o vírus foi encontrado. Por exemplo, se o VirusScan encontrar um arquivo infectado em T:\MEUS DOCUMENTOS e for especificada a pasta INFECTADO como o diretório de quarentena, o programa copiará o arquivo para T:\INFECTADO.

  Você pode digitar um nome na caixa de texto mostrada, ou clicar em **Procurar** para localizar uma pasta adequada no disco rígido.

- **Limpar arquivos infectados automaticamente.** Escolha esta opção para informar ao VirusScan que remova o código do vírus do arquivo infectado assim que for encontrado. Se o VirusScan não puder remover o vírus, a ocorrência será incluída no arquivo de registro se você tiver ativado esse recurso de relatório. Veja o “Escolhendo opções de Relatório” na página 175 para obter mais detalhes.

- **Excluir arquivos infectados automaticamente.** Escolha esta opção para que o VirusScan exclua imediatamente os arquivos infectados encontrados. Certifique-se de ter ativado o recurso de relatório para que você tenha um registro de quais arquivos o programa excluiu. Será necessário restaurar os anexos excluídos a partir de cópias de backup.

- **Continuar a varredura.** Escolha esta opção apenas quando você pretende afastar-se de seu computador enquanto o VirusScan examina-o para buscar vírus. Se as opções de relatório também estiverem ativadas, o programa (veja “Escolhendo opções de Relatório” na página 175 para obter mais detalhes), registrará os nomes dos vírus e os nomes de arquivos infectados para que você possa excluí-los na próxima oportunidade.

3. Clique na guia Alerta para escolher opções adicionais de configuração do VirusScan.

   Para iniciar uma operação de varredura imediatamente apenas com as opções escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar como padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Escolhendo opções de Alerta

Após ser configurado com as opções de ação desejadas, o VirusScan irá procurar vírus no sistema e remover automaticamente os encontrados, sem quase nenhuma outra intervenção. Se, contudo, for possível configurar o VirusScan para avisar-lhe imediatamente após encontrar um vírus, a fim de que você possa realizar a ação necessária, há várias maneiras de configurá-lo para enviar uma mensagem de alerta para você. Use a página de propriedades Alerta para escolher quais métodos de alerta você deseja utilizar.

Siga estas etapas:

1. Clique na guia Alerta na janela do VirusScan Advanced para exibir a página de propriedades correta (Figura 5-14).
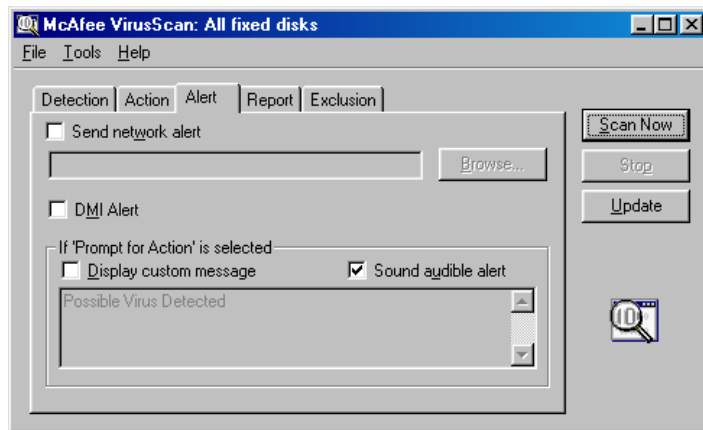
Figura 5-14. VirusScan Advanced - página Alerta

2. Para informar ao VirusScan que envie uma mensagem de alerta a um servidor que esteja executando o NetShield, uma solução antivírus com base em servidor da Network Associates, marque a caixa de verificação **Enviar alerta de rede**, em seguida, digite o caminho para a pasta de alertas do NetShield na sua rede, ou clique em **Procurar** para localizar a pasta correta.

   NOTA: A pasta escolhida deve conter o CENTALRT.TXT, o arquivo Alerta Centralizado do NetShield. Esse programa coleta as mensagens de alerta do VirusScan e de outros softwares da Network Associates, em seguida, as passa para os administradores de rede a fim de que realizem as ações necessárias. Para saber mais sobre o Alerta Centralizado, veja o *Guia do Usuário* do NetShield.

3. Para que o VShield envie mensagens de alerta sobre vírus através da interface de componente DMI para a área de trabalho e os aplicativos de gerenciamento de rede que estejam sendo executados na rede, marque a caixa de verificação **Alerta DMI**.

NOTA: A Desktop Management Interface é um padrão para comunicação de solicitações de gerenciamento e informações sobre alertas entre componentes de hardware e software armazenados em ou conectados a computadores de mesa, e os aplicativos utilizados para gerenciá-los. Para saber mais sobre a utilização desse método de alerta, consulte o administrador de rede.

4. Se você escolher **Solicitar ação ao usuário** como a sua opção na página Ação (veja “Escolhendo opções de Ação” na página 171 para obter mais detalhes), também poderá informar ao VirusScan que emita um sinal sonoro e exiba uma mensagem personalizada ao encontrar um vírus. Para fazer isso, marque a caixa de verificação **Exibir mensagem personalizada** em seguida, digite a mensagem que aparecerá na caixa de texto mostrada — pode ser digitada uma mensagem com 225 caracteres, no máximo. Depois, marque a caixa de verificação **Soar alerta audível**.

5. Clique na guia Relatório para escolher opções adicionais de configuração do VirusScan.

   Para iniciar uma operação de varredura imediatamente apenas com as opções escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar como padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Escolhendo opções de Relatório

O VirusScan cria uma lista com as configurações atuais e resume todas as ações efetuadas, durante as operações de varredura, em um arquivo de registro chamado VSCLOG.TXT. O programa poderá gravar o registro nesse arquivo ou usar um arquivo de texto criado com qualquer editor de texto. Você pode então abrir e imprimir o arquivo de registro para utilizá-lo posteriormente no VirusScan ou no seu editor de texto.

O arquivo VSCLOG.TXT pode servir como uma importante ferramenta de gerenciamento para controlar a atividade de vírus no sistema e anotar quais configurações foram usadas para detectar e atuar contra as infecções encontradas pelo VirusScan. Você também pode utilizar os relatórios de ocorrências registrados no arquivo para determinar quais arquivos é necessário substituir a partir de cópias de backup, examinar na pasta de quarentena ou excluir do seu computador. Use a página de propriedades Relatório para determinar quais informações o VirusScan incluirá no arquivo de registro.

Para configurar o VirusScan a fim de que registre suas ações em um arquivo de registro, siga estas etapas:

1. Clique na guia Relatório na janela do VirusScan Advanced para exibir a página de propriedades correta (Figura 5-15).

Figura 5-15. VirusScan Advanced - página Relatório

2. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, o VirusScan grava as informações de registro no arquivo VSCLOG.TXT, no diretório de programa do VirusScan. Você pode digitar um nome diferente na caixa de texto mostrada, ou clique em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

3. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o VShield limita o tamanho de arquivo para 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, o VShield apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

4. Marque as caixas de verificação correspondentes às informações que o VirusScan deverá incluir no arquivo de registro. Você optar por gravar quaisquer dessas informações:

   - **Detecção de vírus .** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados, encontrados durante esta sessão de varredura.

- **Limpeza de vírus.** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados dos quais removeu os vírus.
- **Eliminação do arquivo infectado.** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados que ele excluiu do sistema.
- **Movimentação do arquivo infectado.** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados que foram movidos para o diretório de quarentena.
- **Configurações da sessão.** Marque esta caixa de verificação para que o VirusScan faça uma lista das opções escolhidas na caixa de diálogo Propriedades do McAfee VirusScan para cada sessão de varredura.
- **Resumo da sessão.** Marque esta caixa de verificação para que o VirusScan faça um resumo das suas ações durante cada sessão de varredura. As informações do resumo incluem o número de arquivos examinados, o número e o tipo de vírus detectados, o número de arquivos movidos ou excluídos, e outras informações.
- **Data e hora.** Marque esta caixa de verificação para que o VirusScan anexe a data e a hora para cada entrada incluída no registro.
- **Nome do usuário.** Marque esta caixa de verificação para que o VirusScan anexe o nome do usuário conectado ao seu computador no momento que incluir cada entrada de registro.

Para ver o conteúdo do arquivo de registro, inicie o VirusScan, em seguida, escolha **Exibir registro de atividades** no menu arquivo **Arquivo**. Para obter mais informações, veja “Usando os menus do VirusScan” na página 155.

5. Clique na guia Exclusão para escolher opções de configuração do VirusScan opcionais.

Para iniciar uma operação de varredura imediatamente apenas com as opções escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar como padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Escolhendo opções de Exclusão

Muitos dos arquivos armazenados no seu computador não são vulneráveis a infecções por vírus. As operações de varredura que examinam esses arquivos podem ocupar um longo tempo e produzir poucos resultados. Você pode acelerar as operações de varredura informando ao VirusScan que examine os tipos de arquivos suscetíveis a infecções (veja “Escolhendo opções de Detecção” na página 165 para obter mais detalhes) ou instruí-lo para ignorar arquivos ou pastas inteiras que não serão infectados.

Após examinar completamente o sistema, você pode excluir os arquivos e pastas que não são alterados ou que não sejam, normalmente, vulneráveis a infecção por vírus. Você também pode contar com o VShield para fornecer-lhe proteção entre as operações de varredura programadas. Contudo, as operações de varredura regulares, que examinam todas as áreas do computador, são a melhor defesa contra vírus.

Para excluir arquivos ou pastas das operações de varredura, siga estas etapas:

1. Clique na guia Exclusão da janela do VirusScan Advanced para exibir a página de propriedades correta (Figura 5-16).
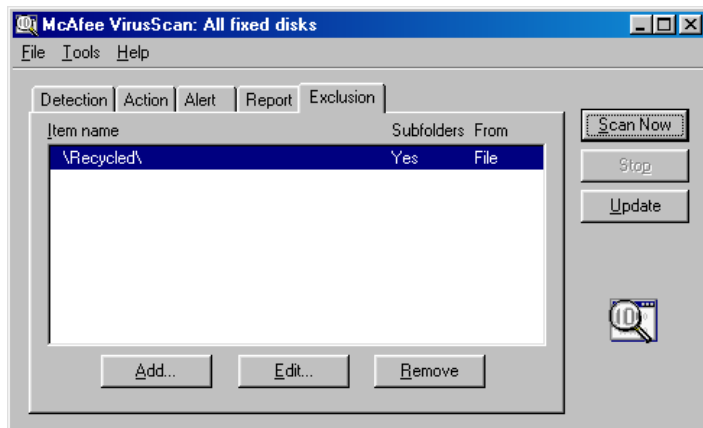
Figura 5-16. Janela do VirusScan Advanced - página Exclusão

A página Exclusão criará inicialmente uma lista com apenas o conteúdo da Lixeira. O VirusScan elimina a Lixeira das operações de varredura porque o Windows não executará os arquivos nela armazenados.

2. Especifique os itens a serem excluídos. Você pode

   - **Adicionar arquivos, pastas e volumes à lista de exclusão.** Clique em **Adicionar** para abrir a caixa de diálogo Adicionar item para exclusão (Figura 5-17).
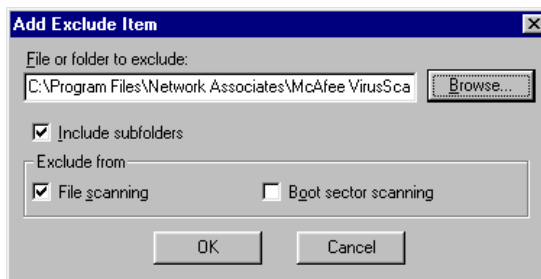
Figura 5-17. Caixa de diálogo Adicionar item para exclusão

a. Caixa de diálogo Adicionar item de exclusão de varredura Digite o volume, o caminho para o arquivo ou para a pasta que você deseja excluir da varredura, ou clique em **Procurar** para localizar um arquivo ou pasta no seu computador.

> **NOTA:** Se você tiver escolhido mover os arquivos infectados para um pasta de quarentena automaticamente, o programa excluirá essa pasta das operações de varredura.

b. Marque a caixa de verificação **Incluir subpastas** para excluir todas as subpastas contidas na pasta especificada.

c. Marque a caixa de verificação **Varredura de arquivo** para informar ao VirusScan que não procure vírus infectantes nos arquivos ou pastas excluídas.

d. Marque a caixa de verificação **Varredura de setor de inicialização** para informar ao VirusScan que não procure vírus de setor de inicialização nos arquivos ou pastas excluídas. Use essa opção para excluir arquivos de sistema, como COMMAND.COM, das operações de varredura.

> **ATENÇÃO:** A Network Associates recomenda que você *não* exclua os seus arquivos de sistema da varredura em busca de vírus.

e. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo.

f. Repita as etapas A a D até incluir na lista todos os arquivos e pastas que não devem ser examinados.

- **Alterar a lista de exclusão.** Para alterar as configurações de um item de exclusão, selecione-o na lista Exclusões, em seguida, clique em **Editar** para abrir a caixa de diálogo Editar item de exclusão de varredura. Faça as alterações necessárias, em seguida, clique em **OK** para fechar a caixa de diálogo.

- **Remover um item da lista.** Para remover um item de exclusão, selecione-o na lista, em seguida, clique em **Remover**. O VirusScan examinará esse arquivo ou pasta durante a próxima operação de varredura.

3. Clique em uma guia diferente para alterar qualquer um dos parâmetros de configuração do VirusScan.

   Para iniciar uma operação de varredura imediatamente apenas com as opções escolhidas, clique em **Examinar agora**. Para salvar as suas alterações como opções de varredura padrão, escolha **Salvar como padrão** no menu **Arquivo** ou clique em **Nova varredura**. Para salvar as suas configurações em um novo arquivo, escolha **Salvar configurações** no menu **Arquivo**, denomine o arquivo na caixa de diálogo mostrada, em seguida, clique em **Salvar**.

Ativando a proteção por senha

O VirusScan permite que você defina uma senha para proteger as suas configurações escolhidas em cada página de propriedades contra alterações não autorizadas. Esse recurso é particularmente útil para administradores de sistemas que precisam impedir que os usuários alterem as suas medidas de segurança modificando os parâmetros do VirusScan. Use a página de propriedades Segurança para bloquear as configurações

---

Para ativar a proteção por senha do VirusScan Advanced, siga estas etapas:

1. Escolha **Proteção por senha** no menu **Ferramentas** na janela do VirusScan Advanced para abrir a caixa de diálogo Proteção por senha (Figura 5-18).
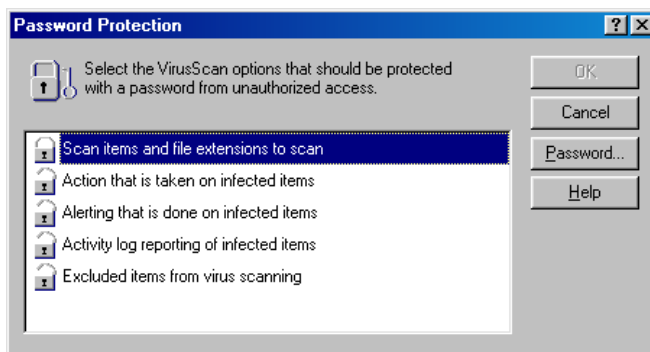
Figura 5-18. Caixa de diálogo Proteção por senha

2. Selecione as configurações que você deseja proteger na lista mostrada.

   Você pode proteger algumas ou todas as páginas de propriedades do VirusScan. As páginas de propriedades protegidas exibem um ícone de um cadeado fechado na lista de segurança mostrada na Figura 5-18. Para remover a proteção de uma página de propriedades, clique no cadeado fechado para abri-lo .

3. Clique em **Senha** para abrir a caixa de diálogo Especificar senha (Figura 5-19).
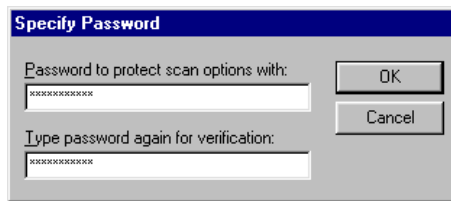
Figura 5-19. Caixa de diálogo Especificar senha

   a. Digite uma senha na primeira caixa de texto mostrada, em seguida, digite a mesma senha novamente na caixa de texto abaixo da primeira para confirmar a sua escolha.

   b. Clique em **OK** para fechar a caixa de diálogo Especificar senha.

4. Clique em **OK** para retornar à janela do VirusScan Advanced.

Planejando tarefas de varredura 6

O que faz o Programador de Tarefas do VirusScan?

O Programador de Tarefas do VirusScan executa operações de varredura e outras tarefas nas datas e horas que você escolher, ou em intervalos predeterminados. Use o Programador de Tarefas para realizar uma operação de varredura na sua ausência, quando isso causar a menor interrupção no seu trabalho, como parte de uma série de tarefas automatizadas, ou de outro modo que atenda às suas necessidades.

Por que planejar as operações de varredura?

Embora o VirusScan inclua componentes que procuram vírus continuamente ou que permitem o exame do seu sistema quando você quiser, é possível planejar operações de varredura regulares e outras atividades do programa.

- **Defina uma programação periódica para o seu sistema.** Se você quiser controlar a atividade viral recorrente no sistema ou na rede, planeje uma varredura completa do sistema a intervalos periódicos. Os recursos de relatório do VirusScan podem fornecer um relatório completo do número, tipo, tamanho e outras características de qualquer vírus encontrado.

- **Complementar ou substituir a varredura por solicitação.** A Network Associates recomenda que você use o VShield para fazer varreduras em busca de vírus continuamente, mas se o seu ambiente não permitir o uso do VShield ou caso tenha requisitos quanto ao desempenho do sistema, programe operações de varredura freqüentes para evitar infecções. Mesmo que o VShield seja utilizado, o planejamento periódico de varreduras completas do sistema reduz a possibilidade de que arquivos infectados não sejam detectados.

- **Alternar operações de varredura.** As operações de varredura planejadas oferecem a flexibilidade da escolha de diferentes operações para objetivos ou momentos distintos. Se, por exemplo, você quiser usar o VShield para examinar o seu sistema continuamente e examinar unidades de rede mapeadas com menos freqüência, poderá planejar uma tarefa com este objetivo.

O Programador de Tarefas contém um conjunto de tarefas padrão já configurado, mas não está planejado. Esse conjunto inclui tarefas que ativam o VShield quando o computador é iniciado, executam uma tarefa de varredura padrão, examinam a unidade C: e todas as unidades de seu sistema, atualizam os arquivos de programas do VirusScan e dos componentes do programa. É possível ativar uma das tarefas padrão inicialmente ou você poderá criar as suas próprias tarefas para atender aos seus hábitos.

Iniciando o Programador de Tarefas do VirusScan

Para iniciar o Programador de Tarefas do VirusScan, escolha um dos seguintes métodos:

- Clique em **Iniciar**, aponte para **Programas**, em seguida para **McAfee VirusScan**. Em seguida, escolha **Programador de Tarefas do McAfee VirusScan** na lista mostrada; ou

- Inicie o VirusScan Classic, em seguida escolha **Programador de Tarefas** no menu **Ferramentas**. Para saber como iniciar o VirusScan, veja Capítulo 5, “Usando o McAfee VirusScan.”

Ambos os métodos abrem a janela do Programador de Tarefas (Figura 6-1). Uma vez iniciado, o Programador de Tarefas também exibe um pequeno ícone na barra de sistema do Windows. Clique duas vezes nesse ícone para exibir a janela do Programador de Tarefas em primeiro plano.
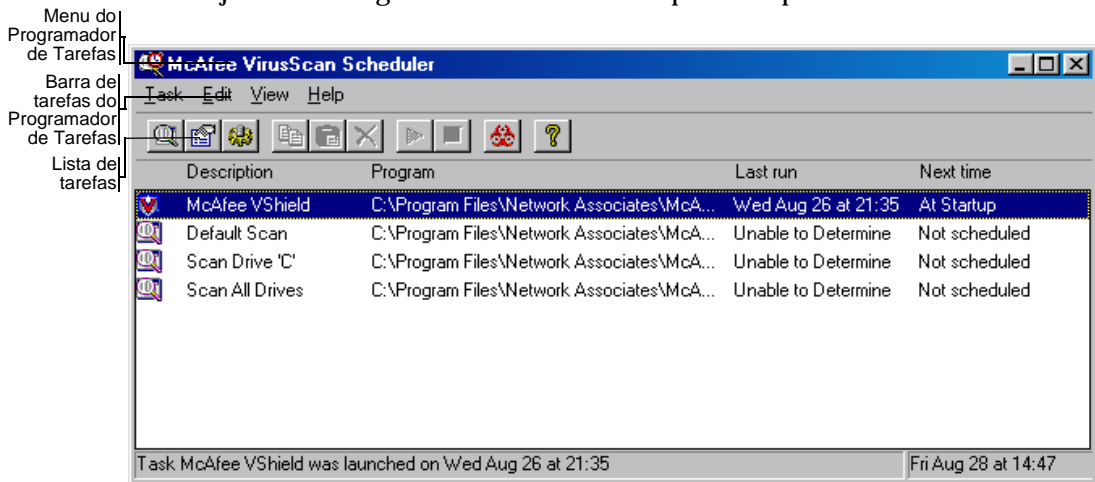
Figura 6-1. Janela do Programador de Tarefas do VirusScan

A janela do Programador de Tarefas mostra inicialmente uma lista de tarefas padrão incluídas nesse componente, predefinidas e prontas para serem executadas. Uma “tarefa” é um conjunto de instruções para executar um determinado programa, com uma configuração específica, em uma hora determinada. A lista de tarefas indica quais programas realizarão a sua tarefa — você irá programar o VShield ou SCAN32.EXE para a maioria delas — exibe a hora e data da última tarefa realizada e mostra quando foi definida para ser reiniciada. Cada nova tarefa criada aparece na parte inferior da lista de tarefas.

A barra de ferramentas, na parte superior da janela do Programador de Tarefas, fornece acesso rápido aos comandos mais comuns do programa. Para exibir apenas os botões dessa barra de ferramentas, clique em **Exibir**, aponte para **Barra de ferramentas**, em seguida escolha **Botões padrão**. Para adicionar legendas aos botões, clique em **Exibir**, aponte para **Barra de ferramentas**, em seguida escolha **Rótulos de texto**. Ambas as opções podem estar ativas ao mesmo tempo — uma marca de seleção ao lado do item do menu indica qual exibição está ativa. Você encontrará a maioria dos comandos da barra de ferramentas nos menus na parte superior da janela do Programador de Tarefas e nos menus de atalho que aparecem ao clicar em uma tarefa da lista com o botão direito do mouse.

Uma barra de status na parte inferior da janela do Programador de Tarefas conta o número de tarefas incluídas na lista. Quando você seleciona uma tarefa na lista, a barra de status informa quando esta foi executada pela última vez. Essa barra mostra também uma descrição breve de cada botão da barra de ferramentas quando o cursor do mouse é deslizado sobre ela. Escolha **Barra de Título** ou **Barra de Status** no menu **Exibir** para mostrar ou ocultar cada elemento da janela.

Usando a janela do Programador de Tarefas

Na janela do Programador de Tarefas, você pode:

- **Programador de Tarefas do VirusScan Criar uma nova tarefa.** Escolha **Nova tarefa** no menu **Tarefa**, ou clique na barra de ferramentas do Programador de Tarefas. Aparecerá uma caixa de diálogo Propriedades da tarefa. Veja “Criando novas tarefas” na página 190 para saber como especificar as ações a serem executadas.

- **Planejar e ativar uma tarefa.** Selecione uma tarefa na lista, na janela do Programador de Tarefas, em seguida, escolha **Propriedades** no menu **Tarefa** ou clique em na barra de ferramentas do Programador de Tarefas. Aparecerá uma caixa de diálogo Propriedades da tarefa. Veja “Ativando tarefas” na página 192 para saber como especificar as opções para a tarefa e prepará-la para ser executada.

- **Configurar o programa da tarefa.** Selecione uma das tarefas na lista da janela do Programador de Tarefas, em seguida, clique em na barra de ferramentas do Programador de Tarefas para exibir uma página de propriedades para o componente de programa do VirusScan que executará a tarefa. A aparência dessa página de propriedades depende de qual componente do VirusScan está em execução. Veja “Configurando opções de tarefas” na página 197 para saber como escolher opções para o programa de varredura.

> **NOTA:** Você pode configurar apenas os programas utilizados para atualizações ou atualização de versão do VirusScan ou aqueles que executam uma operação de varredura — como o VShield ou VirusScan (SCAN32.EXE). Embora seja possível usar o Programador de Tarefas do VirusScan para planejar a execução de outros programas, você não poderá utilizá-lo para *configurar* outros programas.

- **Copiar uma tarefa.** Selecione uma das tarefas na lista da janela do Programador de Tarefas, em seguida, escolha **Copiar** no menu **Editar** ou clique em na barra de ferramentas do Programador de Tarefas. Esse procedimento copia a tarefa para área de transferência do Windows. Em seguida, clique no interior da janela do Programador de Tarefas, depois escolha **Colar** no menu **Editar** ou clique em na barra de ferramentas desse componente, para colar uma cópia da tarefa na lista do Programador de Tarefas. Use esse recurso para copiar as configurações da tarefa que você deseja usar como modelos para outras semelhantes.

- **Excluir uma tarefa.** Selecione uma das tarefas da lista, na janela do Programador de Tarefas, em seguida, escolha **Excluir** no menu **Tarefa**, ou clique em na barra de ferramentas do Programador de Tarefas.

> **NOTA:** Você pode excluir apenas as tarefas que criou — as tarefas do conjunto padrão incluído no Programador de Tarefas não podem ser eliminadas. Você pode, contudo, desativar qualquer tarefa padrão que não queira executar. Veja “Ativando tarefas” na página 192 para obter mais detalhes.

- **Iniciar uma tarefa.** Selecione uma das tarefas da lista, na janela do Programador de Tarefas, em seguida, escolha **Iniciar** no menu **Tarefa** ou clique em na barra de ferramentas do Programador de Tarefas. A tarefa selecionada será iniciada imediatamente e executará com as opções escolhidas. Para ativar as funções de varredura do VShield, selecione McAfee VShield na lista de tarefas, em seguida escolha **Ativar** no menu **Tarefa**. Para iniciar o VShield e carregá-lo na memória, selecione a tarefa VShield, em seguida, clique em na barra de ferramentas do Programador de Tarefas.

- **Parar uma tarefa.** Selecione uma das tarefas na lista da janela do Programador de Tarefas, em seguida escolha **Parar Agora** no menu **Tarefa** ou clique em na barra de ferramentas do Programador de Tarefas. Para parar a execução do VShield, selecione McAfee VShield na lista de tarefas, em seguida, clique em na barra de ferramentas do Programador de Tarefas. Para desativar apenas o VShield, selecione a tarefa VShield, em seguida, escolha **Desativar** no menu **Tarefa**. Para saber como parar o VShield completamente e removê-lo da memória, veja "Desativando ou parando o VShield" na página 147.

- **Conecte-se à Biblioteca de informações sobre vírus da Network Associates.** Escolha **Lista de vírus** no menu **Exibir**, ou clique em na barra de ferramentas do Programador de Tarefas. O VirusScan iniciará o seu aplicativo de navegador preferido e estabelecerá a conexão com o site da web da Network Associates. Veja "Exibindo informações sobre o arquivo e o vírus" na página 79 para saber mais sobre quais informações serão encontradas na biblioteca.

> **NOTA:** Para conectar-se à Biblioteca de informações sobre vírus, você deve ter uma conexão com a Internet e um software de navegador disponível em seu computador.

- **Abrir o arquivo da ajuda online.** Escolha **Tópicos da Ajuda** no menu **Ajuda** ou clique em na barra de ferramentas do Programador de Tarefas para ver uma lista dos tópicos da ajuda do VirusScan.

- **Exibir um Registro de Atividades.** Selecione uma das tarefas na lista da janela do Programador de Tarefas. em seguida escolha **Exibir Registro de Atividades** no menu **Tarefa**. Nem todas as tarefas terão um arquivo de registro associado, mas o VirusScan o abrirá, quando existir, em uma janela do Bloco de Notas (veja Figura 5-2 na página 157). Esse arquivo pode ser editado e copiado como qualquer outro de texto comum. Para saber mais sobre quais informações estão incluídas em cada arquivo de registro, veja Capítulo 4, “Usando o VShield,” e Capítulo 5, “Usando o McAfee VirusScan.”

- **Iniciar o Programador de Tarefas do VirusScan automaticamente.** Escolha **Carregar ao Inicializar** no menu **Exibir** para que o Programador de Tarefas do VirusScan seja iniciado sempre que você ligue o computador. O padrão é essa opção estar ativada no Programador de Tarefas. Como o programa deve estar em execução para executar qualquer tarefa planejada, defina-o para iniciar automaticamente a fim de que as tarefas programadas comecem nos horários agendados.

- **Sair do Programador de Tarefas do VirusScan.** Escolha **Sair** no menu **Tarefa** para sair do Programador de Tarefas. Se houver tarefas pendentes, o programa deve ser minimizado em vez de encerrado. Para saber como reiniciar o Programador de Tarefas, veja “Iniciando o Programador de Tarefas do VirusScan” na página 184.

Programador de Tarefas do VirusScan

Trabalhando com tarefas padrão Logo após instalar o VirusScan no seu computador e reiniciá-lo, o VShield começará imediatamente a examinar o sistema usando uma configuração padrão que lhe fornece um nível de proteção básico. As outras tarefas da lista, na janela do Programador de Tarefas, também apresentam uma configuração padrão, mas essas tarefas permanecem inativas até que sejam ativadas. Veja o “Ativando tarefas” na página 192 para obter mais detalhes.

Estas são as tarefas padrão:

- **VShield.** Como padrão, essa tarefa é executada automaticamente assim que você inicia o seu computador. Não é possível programar o VShield para execução em qualquer outro momento, mas você pode escolher opções de varredura diferentes. Veja “Configurando as propriedades do VShield” na página 91 para saber quais opções estão disponíveis.

- **Examinar Meu Computador.** Essa tarefa examina todos os discos rígidos e toda a mídia removível do sistema, além da RAM e dos setores de inicialização do disco rígido. Você deve ativá-la para que entre em execução. Você pode executar essa tarefa com a sua configuração padrão ou aprender como definir as suas definições padrão — veja "Configurando o VirusScan para varredura planejada" na página 197.

- **Examinar a unidade C:.** Essa tarefa examina a unidade C: , a memória RAM e os setores de inicialização do disco rígido como padrão. Você deve ativá-la para que entre em execução. É possível executá-la com a sua configuração padrão ou aprender como definir as suas configurações — veja "Configurando o VirusScan para varredura planejada" na página 197.

- **Varredura padrão.** Essa tarefa serve como um modelo que pode ser usado para criar outras tarefas. Como padrão, ela examina a unidade C:, a memória RAM e os setores de inicialização do disco rígido. Você deve ativá-la para que entre em execução. É possível executá-la com a configuração padrão ou aprender como definir as suas definições padrão — veja "Configurando o VirusScan para varredura planejada" na página 197.

- AutoUpdate. Essa tarefa estabelece a conexão com um servidor ou site do File Transfer Protocol (FTP) que você designe para atualizar os seus arquivos (.DAT) de dados do VirusScan. A tarefa está configurada para conectar-se ao servidor da Network Associates, mas é necessário programar e ativá-la para que a tarefa atualize os seus arquivos. Você também pode configurar a tarefa para estabelecer a conexão com um servidor central ou site do FTP na sua rede para atualizar os arquivos. Veja "Configurando as opções do AutoUpdate" na página 217 para saber como configurar essa tarefa de modo a atender às suas necessidades.

- AutoUpgrade. Essa tarefa estabelece a conexão com um servidor ou site do File Transfer Protocol (FTP) que você designar para atualizar os componentes de programa do VirusScan para as versões mais recentes. A tarefa deve ser configurada para estabelecer a conexão com um servidor ou site do FTP específico, em seguida deve ser programada e ativada para que atualize a versão dos seus arquivos. Veja "Configurando as opções do AutoUpgrade" na página 230 para saber como configurar a tarefa de modo a atender às suas necessidades.

Criando novas tarefas

Embora as tarefas do conjunto padrão possam fornecer uma proteção adequada ao seu sistema, convém criar e executar as suas próprias tarefas para tornar-se mais experiente com o VirusScan, para ter uma idéia precisa do que e quando deseja que o programa faça uma varredura.

Para criar uma nova tarefa, siga estas etapas:

1. Escolha **Nova Tarefa** no menu **Tarefa** na janela do Programador de Tarefas ou clique em [ícone] na barra de ferramentas do Programador de Tarefas.

   Aparecerá a caixa de diálogo Propriedades da tarefa (Figura 6-2).
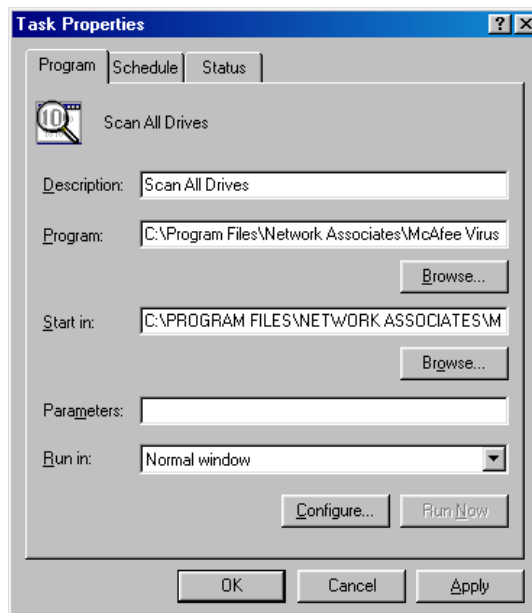
Figura 6-2. Caixa de diálogo Propriedades da tarefa – página Programa

2. Digite um nome para a tarefa na caixa de texto **Descrição**. Certifique-se de que esse nome descreva a tarefa, para que você possa diferenciá-la das outras na janela do Programador de Tarefas e saber imediatamente o que ela faz.

3. Digite o caminho completo e o nome de arquivo do programa que irá realizar a sua tarefa na caixa de texto **Programa** ou clique em **Procurar** para localizá-la no seu disco rígido.

   Como padrão, o Programador de Tarefas escolhe o VirusScan como o programa que executará a tarefa e o localiza no seguinte caminho:

   C:\Program Files\Network Associates\McAfee VirusScan\SCAN32.EXE

   É possível executar qualquer programa executável a partir do Programador de Tarefas do VirusScan, mas você pode configurar as opções do programa somente para o VirusScan, VShield, AutoUpdate e AutoUpgrade. Veja “Configurando opções de tarefas” na página 197 para obter mais detalhes.

4. Para que o programa escolhido na Etapa 3 procure uma pasta específica para seus arquivos de dados, arquivos .INI ou outros itens necessários à inicialização, digite o caminho para a pasta correta na caixa de texto **Iniciar em** ou clique em **Procurar** para localizá-la no seu disco rígido. Normalmente, um programa procurará os arquivos necessários na sua própria pasta.

5. Digite quaisquer parâmetros que o programa deverá usar ao iniciar. Para a maioria dos programas, os parâmetros permitidos incluem quaisquer opções de linha de comando ou qualquer arquivo a ser aberto pelo programa ao iniciar.

6. Escolha **Normal** na lista **Iniciar em** para que o programa apareça na sua janela padrão ao iniciar. Escolha **Maximizado** para expandir até o tamanho máximo. Escolha **Minimizado** para reduzir a janela a um ícone na barra de tarefas.

Nesse ponto, você já inseriu informações suficientes para criar a sua tarefa, mas ainda não foram escolhidas as opções do programa ou um planejamento para a execução. Você pode

- Clicar em **Aplicar** para salvar suas alterações sem fechar a caixa de diálogo Propriedades da tarefa, em seguida, clique na guia Planejar. Para saber como definir um planejamento de tarefa, veja “Ativando tarefas.”

- Clique em **OK** para salvar as suas alterações e retornar à janela do Programador de Tarefas do VirusScan. Você precisará configurar um planejamento de tarefa posteriormente para executá-la. Para fazer isso, selecione a tarefa na lista da janela do Programador de Tarefas, em seguida, clique em para abrir a caixa de diálogo Propriedades da tarefa.
- Clique em **Cancelar** para fechar a caixa de diálogo sem criar uma tarefa.

Ativando tarefas

Ativar uma tarefa significa escolher um planejamento para ela e ativar o planejamento para que entre em execução quando for necessário.
Para executar tarefas que utilizem o VirusScan — mas não o VShield — para examinar o sistema, será preciso também configurar as operações de varredura para que sejam iniciadas automaticamente. Veja Etapa 4 na página 204 para obter mais detalhes.

Para ativar uma tarefa, siga estas etapas:

1. Se a caixa de diálogo Propriedades da tarefa ainda não estiver aberta, clique duas vezes em uma das tarefas da lista, na janela do Programador de Tarefas ou selecione uma tarefa, em seguida, clique em na barra de ferramentas do Programador de Tarefas.

   Aparecerá a caixa de diálogo Propriedades da tarefa (veja a Figura 6-2 na página 190). Se você escolher o VShield, AutoUpdate ou AutoUpgrade na lista de tarefas do Programador de Tarefas, a caixa de diálogo Propriedades da Tarefa terá uma aparência um pouco diferente da que é mostrada na Figura 6-2.

2. Clique na guia Programador de Tarefas para exibir a página de propriedades correta (Figura 6-3 na página 193).

NOTA: A caixa de diálogo Propriedades da Tarefa para o VShield não incluirá a página de Propriedades do Programador de Tarefas — em vez disso, incluirá as páginas de status para cada um dos módulos de varredura do VShield. As caixas de diálogo Propriedades da tarefa para o AutoUpdate e AutoUpgrade, enquanto isso, não conterão as páginas de status.
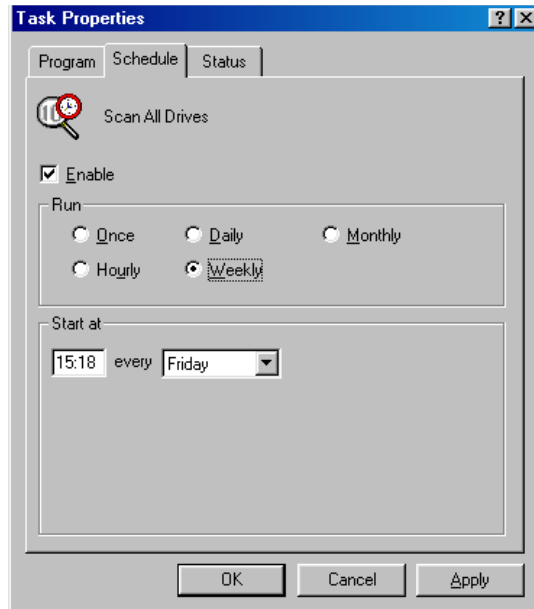
Figura 6-3. Caixa de diálogo Propriedades da tarefa – página Planejamento

3. Marque a caixa de verificação **Ativar**. As opções nas áreas **Executar** e **Iniciar em** são ativadas.

4. Escolha a freqüência de execução da tarefa na área **Executar**. Dependendo do intervalo selecionado, a área **Iniciar em** apresentará um conjunto de opções diferente para o planejamento da tarefa. Estas são as opções:

   - **Uma vez.** Esta opção executa a sua tarefa exatamente uma vez na data e hora especificada. Digite o horário na caixa de texto na extremidade esquerda, na área **Iniciar em**, em seguida, selecione um mês na lista à direita. Depois, digite o dia e o ano nas caixas de texto mostradas.

   - **A cada hora.** Essa opção executa a tarefa a cada hora, se o computador estiver ligado e o Programador de Tarefas em execução. Especifique, na caixa de texto mostrada, quantos minutos o Programador de Tarefas deve aguardar, após cada hora, até executar a tarefa.

- **Diariamente**. Essa opção executa a tarefa uma vez, na hora especificada e nos dias indicados. Digite o horário na caixa de texto mostrada, em seguida, selecione as caixas de verificação para cada dia em que a tarefa será executada.
- **Semanalmente.** Essa opção executa a tarefa uma vez por semana, no dia e na hora especificados. Digite o horário na caixa de texto mostrada, em seguida, escolha um dia na lista à direita.
- **Mensalmente.** Essa opção executa a tarefa uma vez por mês, no dia e na hora especificados. Digite o horário na caixa de texto na extremidade esquerda, em seguida, digite o dia do mês, no qual a tarefa será executada.

NOTA: Digite todos os horários planejados, exceto o intervalo correspondente a cada hora, usando um relógio de 24 horas. Se você quiser que a tarefa seja executada às 9:30 da noite, por exemplo, digite 21:30.

5. Marque a caixa de verificação **Início aleatório em uma hora** para que a tarefa seja iniciada em um ponto aleatório dentro de 60 minutos a partir da hora escolhida como o momento de execução planejada. Por exemplo, suponha que você especificou um intervalo diário e definiu a sua tarefa para ser executada à 1:15 de cada dia. A escolha dessa opção indica ao Programador de Tarefas que a tarefa deve ser executada em qualquer momento entre 1:15 e 2:14.

   Com essa opção ativada, é possível criar e distribuir um arquivo de configuração (.VSC) comum do VirusScan em sua rede, planejar o mesmo conjunto de tarefas para ser executado no mesmo horário, porém mantendo o volume de tráfego na rede em um nível controlado em qualquer ponto. Se a opção estiver desativada, a utilização do mesmo arquivo .VSC para todos os computadores na rede poderá fazer com que cada um deles ative uma tarefa de varredura ou de atualização na mesma hora, o que poderia drenar a largura de banda de rede disponível.

6. Agora, você configurou um planejamento para a tarefa e ela está pronta para ser executada no momento especificado. Clique em **OK** para fechar a caixa de diálogo Propriedades da tarefa ou clique em **Aplicar** para salvar as configurações sem fechar a caixa de diálogo. Clique em **Cancelar** para fechar a caixa de diálogo sem salvar as alterações.

   NOTA: Para iniciar a tarefa, o seu computador deve estar ligado e o Programador de Tarefas do VirusScan em execução. Caso contrário, quando a tarefa tiver que iniciar, será iniciada no próximo horário planejado. Você pode minimizar o Programador de Tarefas a fim de que apareça como um ícone na barra de tarefas do Windows.

   Se você planeja que o VirusScan execute uma tarefa de varredura em um computador desacompanhado, deverá também configurar o programa para iniciar essa operação automaticamente. Veja a Etapa 4 na página 204 para obter mais detalhes.

Verificando o status da tarefa

A janela do Programador de Tarefas do VirusScan faz um resumo da hora e data em que a tarefa foi executada pela última vez e quando foi programada para reiniciar — procure essas informações à direita de cada tarefa na lista. Para ver os resultados de cada tarefa — quantos arquivos foram examinados, se encontrou arquivos infectados e quais ações foram realizadas para reagir às infecções — siga estas etapas para abrir a caixa de diálogo Propriedades da tarefa na página Status.

1. Se a caixa de diálogo Propriedades da tarefa ainda não estiver aberta, clique duas vezes em uma das tarefas da lista, na janela do Programador de Tarefas ou selecione uma tarefa, em seguida, clique em na barra de ferramentas do Programador de Tarefas.

2. Aparecerá a caixa de diálogo Propriedades da tarefa (veja a Figura 6-2 na página 190). Clique na guia Status para exibir a página de propriedades correta (Figura 6-4 na página 196).
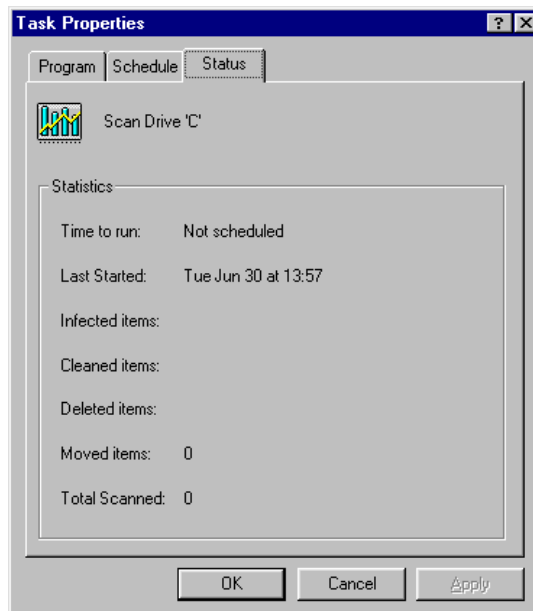
Figura 6-4. Caixa de diálogo Propriedades da tarefa – página Status

A página de status fará uma lista dos resultados da última operação de varredura dessa tarefa e especificará o nome do último arquivo examinado. Clique em **OK** ou **Cancelar** para fechar a caixa de diálogo.

NOTA: A caixa de diálogo Propriedades da tarefa incluirá as páginas de status para todos os módulos de varredura do VShield , porém na mesma caixa para o AutoUpdate e AutoUpgrade essas páginas de status não serão incluídas. Para saber mais sobre a localização de informações de status para o VShield, veja "Controlando informações de status do VShield" na página 151.

Configurando opções de tarefas

Quando uma tarefa é criada e planejada pela primeira vez, o Programador de Tarefas do VirusScan executará o programa especificado na caixa de diálogo Propriedades da tarefa, com um conjunto de opções padrão. Na maioria dos casos, o conjunto padrão fornecerá ao seu computador a proteção suficiente contra vírus e outros softwares destrutivos ou atualizará os arquivos de dados no servidor correto, mas é possível escolher opções personalizadas que respondam melhor aos seus hábitos de trabalho e as necessidades de segurança.

NOTA: O Programador de Tarefas pode ser usado para configurar apenas os componentes de programas do VirusScan. Para configurar qualquer outro software que seja executado a partir do Programador de Tarefas, você deve usar as ferramentas adequadas a este software para configurá-lo separadamente. Consulte a documentação do outro software para obter mais detalhes.

Normalmente, o VirusScan será utilizado para executar as suas tarefas de 9varredura planejadas. Embora seja possível configurar o VShield para realizar várias tarefas de varredura, você não pode especificar quando entrará em execução — o VShield é iniciado quando o computador é ativado e pára a execução quando o computador é desligado. Esse programa pode ser ativado e desativado no Programador de Tarefas, mas você não poderá criar uma segunda tarefa para o VShield.

Configurando o VirusScan para varredura planejada

Para executar uma tarefa de varredura planejada, o VirusScan precisa saber o que deve examinar, ignorar, o que fazer quando encontrar um vírus e como deve informá-lo do ocorrido. Você também deve instruir o VirusScan para criar um registro de suas ações e impedir que outras pessoas alterem as suas configurações. Uma série de páginas de propriedades controla as opções para cada tarefa — clique em cada guia na caixa de diálogo Propriedades do McAfee VirusScan para configurar o programa para a tarefa.

Para trabalhar com as páginas de propriedades do VirusScan, selecione uma das tarefas de varredura na lista da janela do Programador de Tarefas, em seguida clique na barra de ferramentas do programa.

NOTA: A tarefa selecionada deve estar configurada para executar o VirusScan. Você pode modificar uma das tarefas padrão ou configurar uma tarefa que tenha criado. Veja "Criando novas tarefas" na página 190 para saber como especificar o programa que executará a sua tarefa de varredura.

Aparecerá a caixa de diálogo Propriedades do McAfee VirusScan (Figura 6-5).
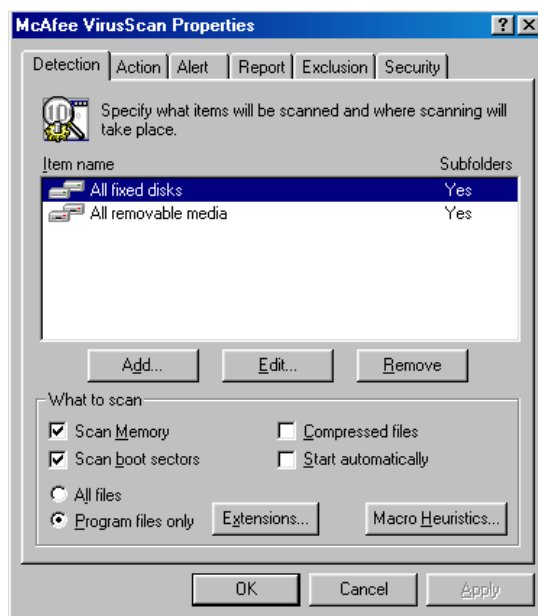
Figura 6-5. Caixa de diálogo Propriedades do VirusScan – página Detecção

Escolhendo opções de detecção

Se você optar por configurar uma tarefa recém-criada, o VirusScan assume inicialmente que a unidade C: e a memória do computador foram escolhidos para serem examinados em busca de vírus de setor de inicialização e que deve restringir a varredura dos arquivos àqueles suscetíveis a infecção por vírus. Se quiser configurar uma das tarefas padrão, as suas opções iniciais poderão variar.

Para modificar as opções iniciais da tarefa, siga estas etapas:

1. Escolha quais partes do sistema ou da rede o VirusScan examinará para procurar vírus. Você pode

   - **Adicionar destinos de varredura.** Clique em **Adicionar** para abrir a caixa de diálogo Adicionar item de varredura (Figura 6-6).
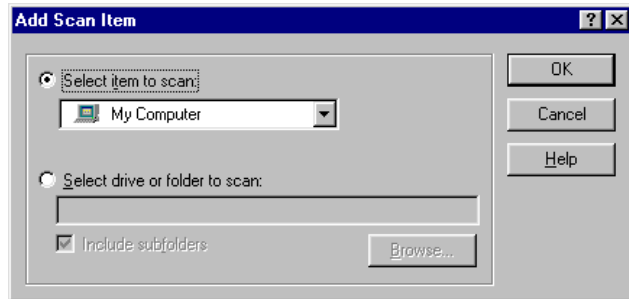
Figura 6-6. Caixa de diálogo Adicionar item de varredura

Para que o VirusScan examine o computador inteiro ou um subconjunto de unidades no sistema ou na rede, clique no botão **Selecionar item para varredura**, em seguida, escolha o destino da varredura na lista fornecida. Estas são as opções:

– **Meu Computador.** Esta opção informa ao VirusScan para examinar todas as unidades fisicamente anexadas ao computador ou logicamente mapeadas através do Windows Explorer para uma letra de unidade no seu computador.

– **Toda a mídia removível.** Esta opção informa ao VirusScan para examinar somente discos de CD-ROM, cartuchos da Syquest e Iomega, ou dispositivos de armazenamento semelhantes anexados fisicamente ao computador.

– **Todos os discos rígidos.** Esta opção informa ao VirusScan para examinar discos rígidos conectados fisicamente ao computador.

– **Todas as unidades de rede.** Esta opção informa ao VirusScan para examinar todas as unidades de disco logicamente mapeadas através do Windows Explorer para uma unidade no seu computador.

Para que o VirusScan examine um disco ou pasta específica no sistema, clique no botão **Selecionar unidade ou pasta para examinar**. Em seguida, na caixa de texto mostrada, digite a letra da unidade de disco ou o caminho da pasta que será examinada ou clique em **Procurar** para localizar o destino de varredura no seu computador. Marque a caixa de verificação **Incluir subpastas** para que o VirusScan também procure vírus no interior das pastas do destino de varredura. Clique em **OK** fechar a caixa de diálogo.

- **Alterar destinos de varredura.** Selecione um dos destinos de varredura da lista, em seguida, clique em **Editar** para abrir a caixa de diálogo Editar item de varredura (Figura 6-7).
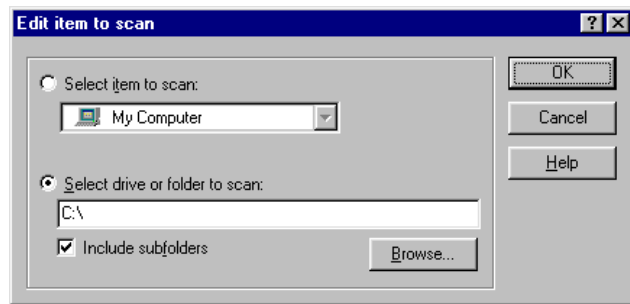
Figura 6-7. A caixa de diálogo Editar item de varredura

A caixa de diálogo aparece com o destino de varredura especificado. Escolha ou digite um novo destino de varredura, em seguida, clique em **OK** para fechar a caixa de diálogo.

- **Remover destinos de varredura.** Selecione um dos destinos de varredura na lista, em seguida, clique em **Remover** para excluí-lo.

2. Especificar quais tipos de arquivos o VirusScan deverá examinar. Você pode

   - **Examinar arquivos compactados.** Marque a caixa de verificação **Arquivos compactados** para que o VirusScan procure vírus em arquivos compactados nos formatos: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Embora proporcione melhor proteção, a varredura de arquivos compactados pode tornar mais lenta uma operação de varredura.

- **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Contudo, você pode reduzir seguramente a abrangência das operações de varredura a esses arquivos mais suscetíveis a infecções por vírus, a fim de acelerá-las. Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou designar as extensões de nomes de arquivos que o VirusScan examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (Figura 6-8).

Figura 6-8. Caixa de diálogo Extensões de arquivo de programa

A caixa de diálogo Extensões de arquivo de programa Como padrão, o VirusScan procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD e .DLL. Os arquivos com as extensões .DO?, .XL?, .RTF e .OBD pertencem ao Microsoft Office, todos esses podem ser infectados por vírus de macros. O ? é um curinga que ativa o VShield para examinar arquivos de documentos e de modelos.

  – Para fazer inclusões na lista, clique em **Adicionar**, em seguida digite as extensões que o VirusScan deverá examinar, na caixa de diálogo mostrada.

  – Para excluir uma extensão da lista, selecione-a, em seguida clique em **Remover**.

  – Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

Para que o VirusScan examine todos os arquivos do seu sistema, com qualquer extensão, selecione o botão **Todos os arquivos**. Embora este procedimento ofereça mais proteção, tornará as operações de varredura consideravelmente mais lentas.

- **Ativar a varredura heurística**. Clique em **Heurística** para abrir a caixa de diálogo Configurações da Varredura Heurística (Figura 6-9).
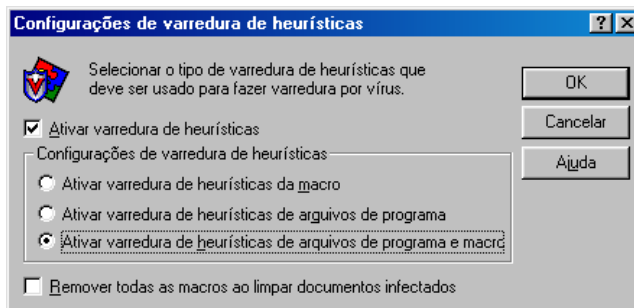
Figura 6-9. Caixa de diálogo Configurações da Varredura Heurística

A tecnologia da varredura heurística possibilita ao VirusScan reconhecer novos vírus com base na sua semelhança com vírus parecidos que o programa já conhece. Para fazê-lo, o VShield procura determinadas características “semelhantes a vírus” nos arquivos que você pediu para serem examinados. A presença de um número suficiente desses elementos. em um arquivo indica ao VShield que marque o arquivo como potencialmente infectado com um vírus novo ou que não foi identificado anteriormente.

Como o VirusScan procura simultaneamente as características de arquivo que descartam a possibilidade de infecção por vírus, raramente será dada uma informação falsa sobre uma infecção. Entretanto, a menos que você saiba que esse arquivo *não* contém um vírus, deverá tratar as infecções “prováveis” com o mesmo cuidado que as confirmadas.

Para ativar a varredura heurística, siga estas etapas

a. Marque a caixa de verificação **Ativar a varredura heurística**. As demais opções na caixa de diálogo são ativadas.

b. Selecione os tipos de varredura heurística que devem ser utilizadas pelo VirusScan. Estas são as opções:

- **Ativar a varredura heurística de macro**. Escolha esta opção para que o. VirusScan identifique todos os arquivos do Microsoft Word, Microsoft Excel e outros do Microsoft Office que tenham macros incorporadas, em seguida compare o código da macro com o banco de dados de assinaturas de vírus. O VirusScan verificará as correspondências exatas com o nome do vírus; as assinaturas de código semelhantes a dos vírus existentes que fazem com que o programa lhe informe que encontrou um provável vírus de macro.
- **Ativar a varredura heurística de arquivos de programa.** Escolha esta opção para que o. VirusScan localize vírus em arquivos de programa examinando as suas características e comparando-as a uma lista de especificações de vírus conhecidos. O programa identificará os arquivos com um número suficiente desses elementos como vírus prováveis.
- **Ativar a varredura heurística de arquivos de programa e macros.** Escolha esta opção para que o. VirusScan use ambos os tipos de varredura heurística. A Network Associates recomenda que você use essa opção para obter uma proteção completa antivírus.

c. Determinar como deseja tratar os arquivos de macros infectados. Selecione **Remover todas as macros ao limpar documentos infectados** para eliminar todos os códigos infectantes do documento e deixar apenas os dados. Para tentar eliminar apenas os códigos de vírus das macros de documentos, não marque essa caixa de verificação.

ATENÇÃO: Use esse recurso com cuidado: a remoção de todas as macros de um documento pode causar a perda de dados ou danificá-lo, tornando o documento inútil.

---

d. Clique em **OK** para salvar as suas configurações e retornar à caixa de diálogo Propriedades do McAfee VirusScan.

3. Escolher outras opções de varredura. Os vírus do setor de inicialização se instalam na memória do seu computador e ocultam-se nos blocos de inicialização ou no registro de inicialização principal do disco rígido. Para detectar esses vírus, marque as caixas de verificação **Examinar a memória** e **Examinar setores de inicialização**.

4. Se você planejou tarefas de varredura que deverão ser executadas quando estiver ausente, marque a caixa de verificação **Iniciar automaticamente** para informar ao VirusScan para começar a varredura logo que seja iniciado. Se esta caixa de verificação não estiver marcada, o Programador de Tarefas iniciará o VirusScan, que aguardará até que você clique em **Examinar agora** para começar a varredura. Se a caixa de verificação for deixada em branco, você terá a chance de cancelar a operação de varredura, caso interfira em seu trabalho.

5. Clique na guia Ação para escolher opções do VirusScan adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do VirusScan, clique em **Aplicar**. Para salvar as alterações e retornar à janela do Programador de Tarefas, clique em **OK**. Para retornar à janela do Programador de Tarefas sem salvar as alterações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Ação

Quando o VirusScan detecta um vírus, poderá lhe perguntar o que deve fazer com o arquivo infectado, ou atuar automaticamente realizando uma ação predeterminada. Use a página de propriedades Ação para especificar quais opções de ação o VirusScan deve lhe propor ao encontrar um vírus ou quais as ações que o programa deve realizar automaticamente.

Siga estas etapas:

1. Para iniciar a partir da janela do Programador de Tarefas, selecione a tarefa criada na lista, em seguida, clique em na barra de ferramentas do Programador de Tarefas.

2. Aparece a caixa de diálogo Propriedades do McAfee VirusScan (veja Figura 6-5 na página 198). Clique na guia Ação na janela do VirusScan Advanced para exibir a página de propriedades correta (Figura 6-10 na página 205).
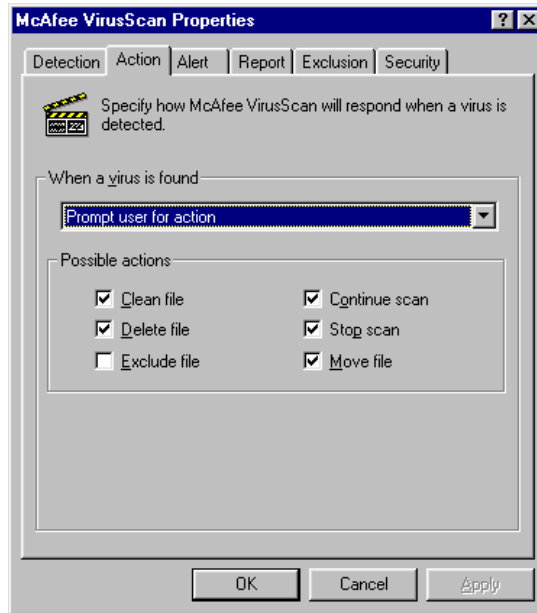
Figura 6-10. Caixa de diálogo Propriedades do VirusScan – página Ação

3. Para informar ao VirusScan o que fazer ao encontrar um vírus, escolha a ação na lista **Quando um vírus for encontrado**. A área imediatamente abaixo da lista será alterada para mostrar as opções adicionais para cada uma delas. Estas são as opções:

   - **Solicitar ação ao usuário.** Use esta opção se você espera estar próximo ao seu computador enquanto o VirusScan examina o disco — VirusScan o programa exibirá uma mensagem de alerta quando encontrar um vírus e lhe proporá a sua ampla gama de opções disponíveis. Escolha as opções de ação que você deseja ver na mensagem de alerta:

     – **Limpar arquivo.** Esta opção informa ao VirusScan para tentar remover o código de vírus do arquivo infectado.

     – **Excluir arquivo.** Esta opção informa ao VirusScan para excluir o arquivo infectado imediatamente.

- **Excluir o item da varredura.** Esta opção informa ao VirusScan para ignorar o arquivo durante as próximas operações de varredura. Esta é a única opção que não é selecionada como padrão.
- **Continuar a varredura.** Esta opção informa ao VirusScan para continuar a varredura, mas não atuar de qualquer outra maneira. Se as opções de relatório estiverem ativadas, o VirusScan incluirá a ocorrência no arquivo de registro.
- **Parar a varredura.** Esta opção informa ao VirusScan que deve parar a operação de varredura imediatamente. Para continuar, você deve reiniciar a operação, no Programador de Tarefas ou no VirusScan.
- **Mover arquivo.** Esta opção informa ao VirusScan para mover o arquivo infectado para um diretório de quarentena.

• **Mover arquivos infectados automaticamente**. Use esta opção para que o VirusScan mova os arquivos infectados para um diretório de quarentena logo após encontrá-los. Como padrão, o VirusScan move esses arquivos para uma pasta chamada INFECTADO, criada no nível raiz da unidade na qual o vírus foi encontrado. Por exemplo, se o VirusScan encontrar um arquivo infectado em T:\MEUS DOCUMENTOS e for especificada a pasta INFECTADO como o diretório de quarentena, o programa copiará o arquivo para T:\INFECTADO.

  Você pode digitar um nome na caixa de texto mostrada, ou clicar em **Procurar** para localizar uma pasta adequada no disco rígido.

• **Limpar arquivos infectados automaticamente.** Use esta opção para informar ao VirusScan para remover o código do vírus do arquivo infectado assim que for encontrado. Se o programa não puder removê-lo, você receberá um aviso através de uma notificação na área de mensagem e, caso os recursos de relatório estiverem ativados, a ocorrência será incluída no arquivo de registro. Veja o “Escolhendo opções de Relatório” na página 209 para obter mais detalhes.

• **Excluir arquivos infectados automaticamente.** Use esta opção para que o VirusScan exclua imediatamente os arquivos infectados encontrados. Certifique-se de ter ativado o recurso de relatório para que você tenha um registro de quais arquivos o programa excluiu. Será necessário restaurar os anexos excluídos a partir de cópias de backup.

- **Continuar a varredura.** Use esta opção apenas se você planeja afastar-se do seu computador enquanto o VirusScan procura vírus. Se as opções de relatório também estiverem ativadas, o programa (veja “Escolhendo opções de Relatório” na página 209 para obter mais detalhes), registrará os nomes dos vírus e os nomes de arquivos infectados para que você possa excluí-los na próxima oportunidade.

4. Clique na guia Alerta para escolher opções do VirusScan adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do VirusScan, clique em **Aplicar**. Para salvar as alterações e retornar à janela do Programador de Tarefas, clique em **OK**. Para retornar à janela do Programador de Tarefas sem salvar as alterações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Alerta

Após configurar o VirusScan com as opções de ação desejadas, você poderá deixá-lo procurar e remover vírus do seu sistema automaticamente, ao encontrá-los necessitando muito pouco da sua interferência. Se, contudo, for possível configurar o VirusScan para avisar-lhe imediatamente após encontrar um vírus, a fim de que você possa realizar a ação necessária, há várias maneiras de configurá-lo para enviar uma mensagem de alerta para você. Use a página de propriedades de Alerta para escolher quais métodos de alerta deseja utilizar.

Siga estas etapas:

1. Para iniciar a partir da janela do Programador de Tarefas, selecione a tarefa criada na lista, em seguida, clique em na barra de ferramentas do Programador de Tarefas.

2. Aparece a caixa de diálogo Propriedades do McAfee VirusScan (veja Figura 6-5 na página 198). Clique na guia Alerta para exibir a página de propriedades correta (Figura 6-11 na página 208).
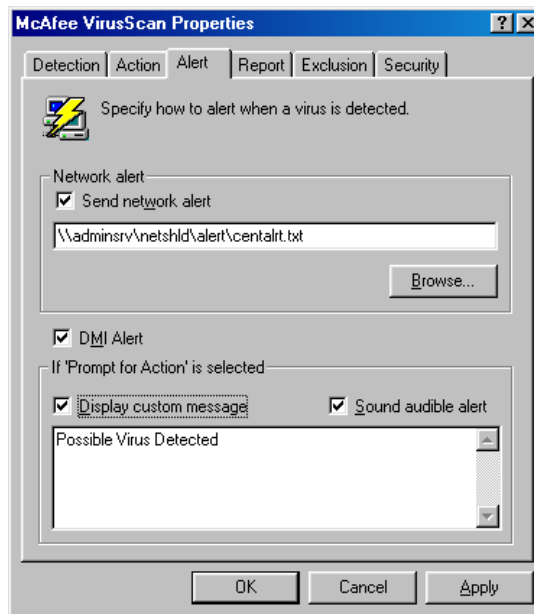
Figura 6-11. Caixa de diálogo Propriedades do VirusScan – página Alerta

3. Para informar ao VirusScan que envie uma mensagem de alerta a um servidor que esteja executando o NetShield, uma solução antivírus com base em servidor da Network Associates, marque a caixa de verificação **Enviar alerta de rede**, em seguida, digite o caminho para a pasta de alertas do NetShield na sua rede, ou clique em **Procurar** para localizar a pasta correta.

   NOTA: A pasta escolhida deve conter o CENTALRT.TXT, o arquivo Alerta Centralizado do NetShield. Esse programa coleta as mensagens de alerta do VirusScan e de outros softwares da Network Associates, em seguida, as passa para os administradores de rede a fim de que realizem as ações necessárias. Para saber mais sobre o Alerta Centralizado, veja o *Guia do Usuário* do NetShield.

4. Para que o VShield envie mensagens de alerta sobre vírus através da interface de componente DMI para a área de trabalho e os aplicativos de gerenciamento de rede que estejam sendo executados na rede, marque a caixa de verificação **Alerta DMI**.

❑ **NOTA:** A Desktop Management Interface é um padrão para comunicação de solicitações de gerenciamento e informações sobre alertas entre componentes de hardware e software armazenados em ou conectados a computadores de mesa, e os aplicativos utilizados para gerenciá-los. Para saber mais sobre a utilização desse método de alerta, consulte o administrador de rede.

5. Se você escolher **Solicitar ação ao usuário** como a sua opção na página Ação (veja "Escolhendo opções de Ação" na página 204 para obter mais detalhes), também poderá informar ao VirusScan que emita um sinal sonoro e exiba uma mensagem personalizada ao encontrar um vírus. Para fazê-lo, marque a caixa de verificação **Exibir mensagem personalizada**, em seguida, digite a mensagem que aparecerá na caixa de texto mostrada — pode ser digitada uma mensagem com 225 caracteres, no máximo. Depois, marque a caixa de verificação **Soar alerta audível**.

6. Clique na guia Relatório para escolher as opções do VirusScan adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do VirusScan, clique em **Aplicar**. Para salvar as alterações e retornar à janela do Programador de Tarefas, clique em **OK**. Para retornar à janela do Programador de Tarefas sem salvar as alterações, clique em **Cancelar**.

❑ **NOTA:** O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Relatório

O VirusScan cria uma lista com as configurações atuais e resume todas as ações efetuadas, durante as operações de varredura, em um arquivo de registro chamado VSCLOG.TXT. O programa poderá gravar o registro nesse arquivo ou usar um arquivo de texto criado com qualquer editor de texto. Esse arquivo de registro pode ser aberto e impresso para revisão posterior no VirusScan ou em qualquer editor de texto.

O arquivo VSCLOG.TXT pode servir como uma importante ferramenta de gerenciamento para controlar a atividade de vírus no sistema e anotar quais configurações foram usadas para detectar e atuar contra as infecções encontradas pelo VirusScan. Você também pode utilizar os relatórios de ocorrências registrados no arquivo para determinar quais arquivos é necessário substituir a partir de cópias de backup, examinar na pasta de quarentena ou excluir do seu computador. Use a página de propriedades Relatório para determinar quais informações o VirusScan incluirá no arquivo de registro.

Para configurar o VirusScan a fim de que registre suas ações em um arquivo de registro, siga estas etapas:

1. Para iniciar a partir da janela do Programador de Tarefas, selecione a tarefa criada na lista, em seguida, clique em na barra de ferramentas do Programador de Tarefas.

2. Aparece a caixa de diálogo Propriedades do McAfee VirusScan (veja Figura 6-5 na página 198). Clique na guia Relatório para exibir a página de propriedades correta (Figura 6-12).
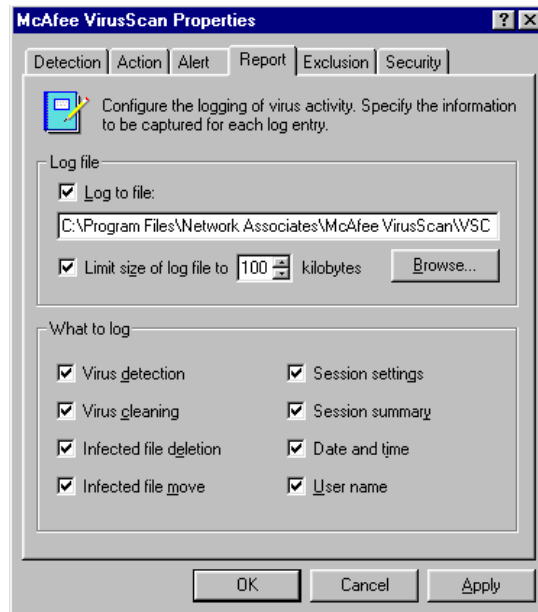
Figura 6-12. Propriedades do VirusScan – página Relatório

3. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, o VirusScan grava as informações de registro no arquivo VSCLOG.TXT, no diretório de programa do VirusScan. Você pode digitar um nome diferente na caixa de texto mostrada, ou clique em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

4. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o VShield limita o tamanho de arquivo para 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, o VShield apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

5. Marque as caixas de verificação correspondentes às informações que o VirusScan deverá incluir no arquivo de registro. Você pode optar por gravar quaisquer dessas informações:

   - **Detecção de vírus.** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados, encontrados durante esta sessão de varredura.

   - **Limpeza de vírus.** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados dos quais removeu os vírus.

   - **Eliminação do arquivo infectado.** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados que ele excluiu do sistema.

   - **Movimentação do arquivo infectado.** Marque esta caixa de verificação para que o VirusScan anote o número de arquivos infectados que foram movidos para o diretório de quarentena.

   - **Configurações da sessão.** Marque esta caixa de verificação para que o VirusScan faça uma lista das opções escolhidas na caixa de diálogo Propriedades do McAfee VirusScan para cada sessão de varredura.

   - **Resumo da sessão.** Marque esta caixa de verificação para que o VirusScan faça um resumo das suas ações durante cada sessão de varredura. As informações do resumo incluem o número de arquivos examinados, o número e o tipo de vírus detectados, o número de arquivos movidos ou excluídos, e outras informações.

   - **Data e hora.** Marque esta caixa de verificação para que o VirusScan anexe a data e a hora para cada entrada incluída no registro.

   - **Nome do usuário.** Marque esta caixa de verificação para que o VirusScan anexe o nome do usuário conectado ao seu computador no momento que incluir cada entrada de registro.

Para ver o conteúdo do arquivo de registro com o Programador de Tarefas do VirusScan, selecione na lista a tarefa que você criou, em seguida escolha **Exibir Registro de Atividades** no menu **Tarefa**. É possível também iniciar o VirusScan e escolher **Exibir Registro de Atividades** no menu **Arquivo**. Para obter mais informações, veja "Usando os menus do VirusScan" na página 155.

6. Clique na guia Exclusão a fim de escolher as opções do VirusScan opcionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do VirusScan, clique em **Aplicar**. Para salvar as alterações e retornar à janela do Programador de Tarefas, clique em **OK**. Para retornar à janela do Programador de Tarefas sem salvar as alterações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Exclusão

Muitos dos arquivos armazenados no seu computador não são vulneráveis a infecções por vírus. As operações de varredura que examinam esses arquivos podem ocupar um longo tempo e produzir poucos resultados. Você pode acelerar as operações de varredura informando ao VirusScan que procure vírus apenas nos tipos de arquivos mais suscetíveis a infecções (veja "Escolhendo opções de detecção" na página 198 para obter mais detalhes) ou indicar ao programa que ignore arquivos ou pastas inteiras que não possam ser infectadas.

Após examinar completamente o sistema, você pode excluir os arquivos e pastas que não são alterados ou que não sejam, normalmente, vulneráveis a infecção por vírus. É possível também confiar no VShield para fornecer-lhe proteção entre as operações de varredura planejadas. Contudo, as operações de varredura regulares, que examinam todas as áreas do computador, são a melhor defesa contra vírus.

Para excluir arquivos ou pastas das operações de varredura, siga estas etapas:

1. Para iniciar a partir da janela do Programador de Tarefas, selecione a tarefa criada na lista, em seguida, clique em [ícone] na barra de ferramentas do Programador de Tarefas.

2. Aparece a caixa de diálogo Propriedades do McAfee VirusScan (veja Figura 6-5 na página 198). Clique na guia Exclusão para exibir a página de propriedades correta. (Figura 6-13).
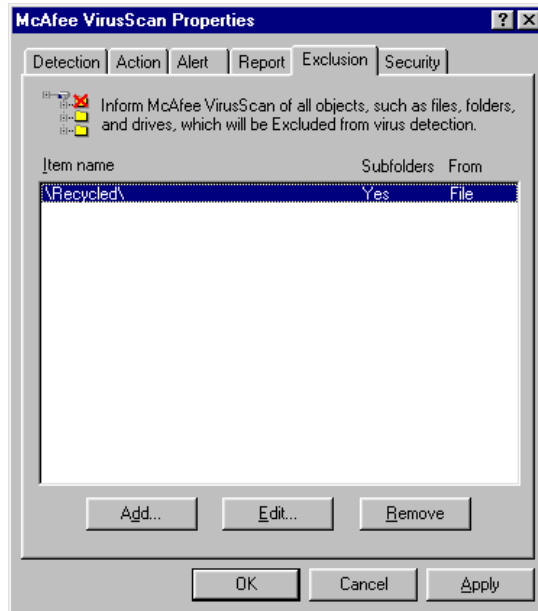
Figura 6-13. Caixa de diálogo Propriedades do VirusScan – página Exclusão

A página Exclusão criará inicialmente uma lista com apenas o conteúdo da Lixeira. O VirusScan elimina a Lixeira das operações de varredura porque o Windows não executará os arquivos nela armazenados.

3. Especifique os itens a serem excluídos. Você pode

   - **Adicionar arquivos, pastas e volumes à lista de exclusão.** Clique em **Adicionar** para abrir a caixa de diálogo Adicionar item para exclusão (Figura 6-14).
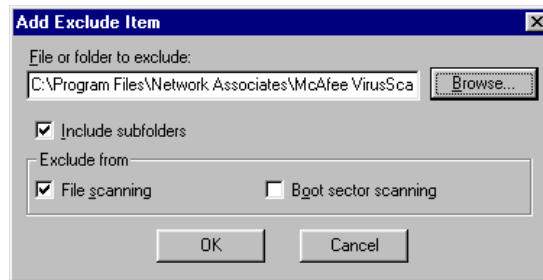
Figura 6-14. Caixa de diálogo Adicionar item para exclusão

a. Caixa de diálogo Adicionar item de exclusão de varredura Digite o volume, o caminho para o arquivo ou para a pasta que você deseja excluir da varredura, ou clique em **Procurar** para localizar um arquivo ou pasta no seu computador.

> **NOTA:** Se você tiver escolhido mover os arquivos infectados para um pasta de quarentena automaticamente, o programa excluirá essa pasta das operações de varredura.

b. Marque a caixa de verificação **Incluir subpastas** para excluir todas as subpastas contidas na pasta especificada.

c. Marque a caixa de verificação **Varredura de arquivo** para informar ao VirusScan que não procure vírus infectantes nos arquivos ou pastas excluídas.

d. Marque a caixa de verificação **Varredura de setor de inicialização** para informar ao VirusScan que não procure vírus de setor de inicialização nos arquivos ou pastas excluídas. Use essa opção para excluir arquivos de sistema, como COMMAND.COM, das operações de varredura.

> **ATENÇÃO:** A Network Associates recomenda que você *não* exclua os seus arquivos de sistema da varredura em busca de vírus.

e. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo.

f. Repita as etapas de a. a d. até completar uma lista com todos os arquivos e pastas que você não deseja que sejam examinadas.

- **Alterar a lista de exclusão.** Para alterar as configurações de um item de exclusão, selecione-o na lista Exclusões, em seguida, clique em **Editar** para abrir a caixa de diálogo Editar item de exclusão de varredura. Faça as alterações necessárias, em seguida, clique em **OK** para fechar a caixa de diálogo.

- **Remover um item da lista.** Para remover um item de exclusão, selecione-o na lista, em seguida, clique em **Remover**. O VirusScan examinará esse arquivo ou pasta durante a próxima operação de varredura.

4. Clique na guia Segurança para escolher opções do VirusScan adicionais. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do VirusScan, clique em **Aplicar**. Para salvar as alterações e retornar à janela do Programador de Tarefas, clique em **OK**. Para retornar à janela do Programador de Tarefas sem salvar as alterações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de segurança

O VirusScan permite que você defina uma senha para proteger as suas configurações escolhidas em cada página de propriedades contra alterações não autorizadas. Esse recurso é particularmente útil para administradores de sistemas que precisam impedir que os usuários alterem as suas medidas de segurança modificando os parâmetros do VirusScan. Use a página de propriedades Segurança para bloquear as configurações

Siga estas etapas:

1. Para iniciar a partir da janela do Programador de Tarefas, selecione a tarefa criada na lista, em seguida, clique em na barra de ferramentas do Programador de Tarefas.

2. Aparece a caixa de diálogo Propriedades do McAfee VirusScan (veja Figura 6-5 na página 198). Clique na guia Segurança para exibir a página de propriedades correta. (Figura 6-15 na página 216).
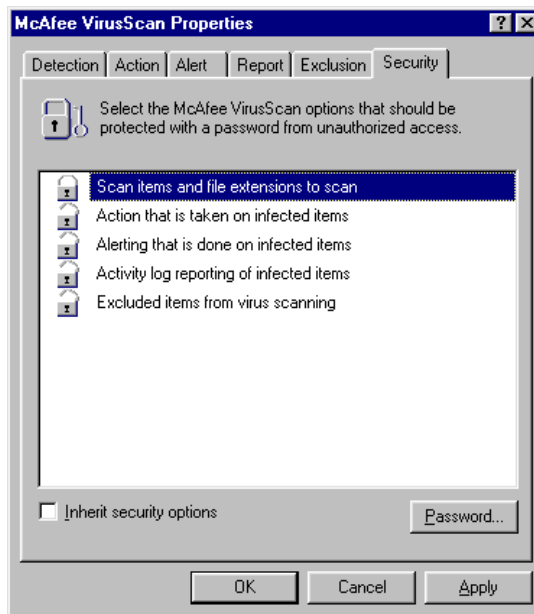
Figura 6-15. Caixa de diálogo Propriedades do VirusScan – página Segurança

3. Selecione as configurações que você deseja proteger na lista mostrada.

   Você pode proteger algumas ou todas as páginas de propriedades do VirusScan. As páginas de propriedades protegidas exibem um ícone de um cadeado fechado na lista de segurança mostrada na Figura 6-15. Para remover a proteção de uma página de propriedades, clique no cadeado fechado para abri-lo .

4. Clique em **Senha** para abrir a caixa de diálogo Especificar senha (Figura 6-16).
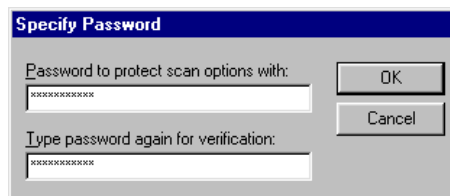
Figura 6-16. Caixa de diálogo Especificar senha

a. Digite uma senha na primeira caixa de texto mostrada, em seguida, digite a mesma senha novamente na caixa de texto abaixo da primeira para confirmar a sua escolha.

b. Clique em **OK** para fechar a caixa de diálogo Especificar senha.

5. Se você quiser outras tarefas de varredura copiando essa tarefa (veja a página 186 para obter mais detalhes), poderá assegurar que as suas configurações aparecerão, como padrão, na tarefa copiada, marcando a caixa de verificação **Herdar opções de segurança**. Se você configurar a tarefa Varredura Padrão com esta opção, todas as novas tarefas criadas escolhendo **Nova Tarefa** no menu **Examinar** ou clicando em terão as definições de segurança selecionadas para a tarefa Varredura Padrão.

6. Clique em uma guia diferente para alterar as suas configurações do VirusScan. Para salvar as alterações sem fechar a caixa de diálogo Propriedades do VirusScan, clique em **Aplicar**. Para salvar as alterações e retornar à janela do Programador de Tarefas, clique em **OK**. Para retornar à janela do Programador de Tarefas sem salvar as alterações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Configurando as opções do AutoUpdate

Para funcionar com máxima eficiência, o VirusScan precisa de inserções regulares de novos arquivos de definição de vírus, atualizações de seu banco de dados de objetos e sites da Internet nocivos, e outras melhorias técnicas. Sem arquivos atualizados, o VirusScan poderá não reconhecer novas formas de software destrutivo ou detectar novos tipos de vírus quando os encontrar.

A Network Associates, através de sua divisão McAfee Labs, atualiza regularmente e com freqüência esses arquivos críticos, tornando os arquivos revistos disponíveis nos seus servidores FTP (File Transfer Protocol) como pacotes de arquivos de dados (.DAT). Um pacote .DAT consiste de arquivo .ZIP para arquivamento chamado DAT-XXXX.ZIP. O XXXX no nome do arquivo é um número serial que é alterado para cada versão do arquivo .DAT.

NOTA: “Atualizar” o VirusScan significa fazer download e instalar novas versões dos arquivos .DAT; “atualizar a versão” do VirusScan significa fazer download e instalar revisões da versão do produto, de executáveis e, em alguns casos, arquivos .DAT. A Network Associates oferece atualizações gratuitas dos arquivos .DAT de dados durante a vida do produto. Porém, isso não garante que esses arquivos serão compatíveis com as versões anteriores do produto.

O seu direito a fazer download grátis de atualizações de versão do VirusScan depende dos termos da sua licença ou do contrato de venda com o qual você concordou no momento da compra do produto. Se você tiver perguntas a fazer sobre esses termos, consulte os documentos LICENSE.TXT ou README.1ST incluídos na sua cópia do VirusScan, ou entre em contato com o seu representante de vendas. A Network Associates torna disponíveis os arquivos de atualização de versão para download grátis nos sites de FTP e outros serviços contanto que a sua licença permita. O Programador de Tarefas do VirusScan usa uma tarefa diferente, o AutoUpgrade, para controlar quando e com que freqüência devem ser obtidos por download os novos arquivos do VirusScan. Veja “Configurando as opções do AutoUpgrade” na página 230 para saber como configurar essa tarefa.

Como padrão, a tarefa AutoUpdate incluída no Programador de Tarefas do VirusScan está configurada para fazer download das atualizações de arquivos .DAT mais recentes no site de FTP da Network Associates. Essa configuração torna simples e direta a administração de redes pequenas .ou instalações individuais do VirusScan. Contudo, se a sua rede for grande, manter essa configuração pode sobrecarregar drasticamente a sua largura de banda externa se, como acontece caso você deixe a configuração padrão ativada, cada nó de rede tentar atualizar seus arquivos de dados .DAT simultaneamente.

Em vez disso, a Network Associates recomenda o uso do AutoUpdate junto com o serviço complementar, Enterprise SecureCast, numa estrutura “push-pull” eficiente. Uma vez instalado o seu software de cliente em um servidor administrativo, o SecureCast pode enviar, ou “push”, os arquivos atualizados para você automaticamente, assim que a McAfee Labs os torne disponíveis. Veja “Configurando o Enterprise SecureCast” na página 283 para obter mais detalhes.

Se você tornar disponíveis esses arquivos atualizados em um ou mais servidores centrais na sua rede e configurar os nós de rede restantes para receber, “pull”, os arquivos atualizados desses servidores, poderá

- Planejar revezamentos de distribuições dos arquivos .DAT em toda a rede para horários convenientes e com uma mínima intervenção de administradores ou usuários de rede. Com a caixa de diálogo Propriedades da tarefa do programador de tarefas do VirusScan, é possível determinar quando cada nó de rede fará consulta seqüencial para procurar arquivos atualizados.

  Você poderia, por exemplo, especificar um horário de atualização conveniente quando distribuir o VirusScan pela primeira vez, mas defina o AutoUpdate para ser acionado em um intervalo aleatório dentro de 60 minutes a partir da hora especificada, ou defina um planejamento periódico ou rotativo de atualizações de arquivos .DAT entre diferentes partes da rede. Para saber como programar o AutoUpdate ou outras tarefas, veja “Ativando tarefas” na página 192.

- Reparta as os serviços de administração periódica entre os diversos servidores e controladores de domínio, entre diferentes áreas das redes remotas ou por todas as outras divisões da rede. A manutenção do tráfego de atualização basicamente interno também pode reduzir as quebras de segurança potenciais de rede.

- Reduzir a probabilidade do tempo de espera necessário para fazer download de novos arquivos .DAT. O tráfego nos servidores da Network Associates aumenta significativamente nas datas de publicação regulares dos arquivos .DAT. Evitar a competição por larguras de banda na rede lhe possibilita distribuir a sua atualização com interrupções mínimas.

Outras opções avançadas do AutoUpdate permitem que você faça backup dos arquivos .DAT existentes, instale a atualização do arquivo .DAT, reinicialize o computador, se for necessário, ou execute programas específicos após atualizações bem-sucedidas. Um conjunto de páginas de propriedades do AutoUpdate controla as opções para essa tarefa — clique em cada guia na caixa de diálogo Propriedades da atualização automática para configurá-las.

Para configurar o AutoUpdate, siga estas etapas:

1. Selecione a tarefa AutoUpdate mostrada na janela do Programador de Tarefas, em seguida em [ícone] na barra de ferramentas do Programador de Tarefas.

NOTA: O AutoUpdate é executado de acordo com o planejamento definido na caixa de diálogo Propriedades da tarefa. Uma alternativa para abrir essa caixa de diálogo é selecionar a tarefa AutoUpdate, em seguida clicar [ícone] na barra de ferramentas do Programador de tarefas. Para saber mais sobre a maneira de definir um planejamento de tarefa, veja "Ativando tarefas" na página 192.

A caixa de diálogo Atualização automática aparecerá (veja Figura 6-17).
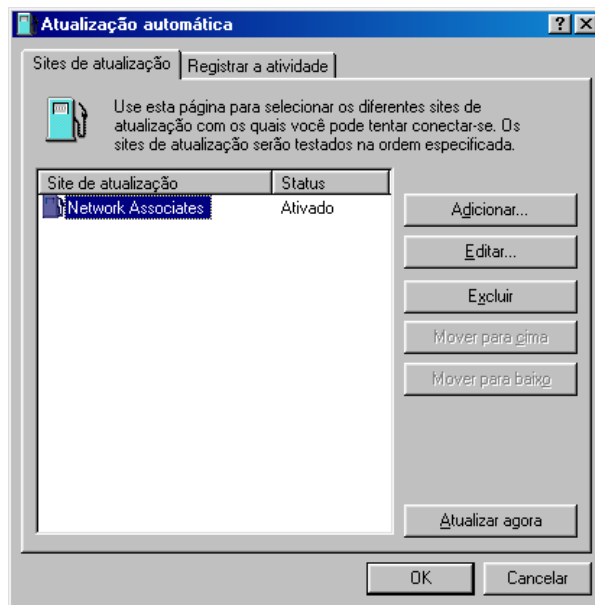
Figura 6-17. Caixa de diálogo Atualização automática - página Atualizar sites

Nessa etapa, o AutoUpdate faz uma lista dos sites dos quais fará download dos novos arquivos .DAT. Inicialmente, o AutoUpdate está configurado para conectar-se apenas com o site de FTP da Network Associates. Você pode adicionar quantos sites forem necessários e alterar a ordem na qual o tenta estabelecer essas conexões a partir dessa caixa de diálogo. Estas são as opções:

- **Adicionar um novo site.** Clique em **Adicionar** para abrir a caixa de diálogo Propriedades da atualização automática (Figura 6-18). Para saber como especificar opções para o novo site, veja "Configurando as opções de atualização" na página 223.
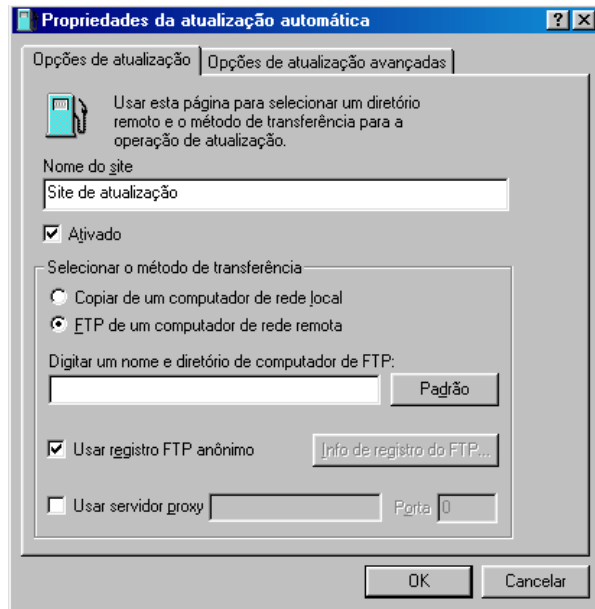
Figura 6-18. Caixa de diálogo Propriedades da atualização automática - página Opções de atualização

- **Alterar as opções para uma tarefa existente.** Selecione um dos sites mostrados na lista, em seguida clique em **Editar** para abrir a caixa de diálogo Propriedades da atualização automática (veja Figura 6-18). Faça as alterações que você quiser, em seguida clique em **OK** para fechar a caixa de diálogo. Para ver as descrições e instruções para configurar as opções disponíveis, veja "Configurando as opções de atualização" na página 223.

- **Remover um site existente.** Selecione um dos sites mostrados na lista, em seguida clique em **Excluir** para removê-lo.

- **Alterar a ordem de pesquisa nos sites existentes.** Para alterar a ordem na qual o AutoUpdate conecta-se aos sites da lista na caixa de diálogo, selecione o site cuja prioridade você deseja alterar, em seguida clique em **Mover para cima** para dar ao site uma prioridade mais alta, ou **Mover para baixo** para dar ao site uma prioridade mais baixa.

- **Atualizar seus arquivos .DAT imediatamente.** Clique em **Atualizar agora** para que o AutoUpdate conecte-se imediatamente ao primeiro site da lista e procure os novos arquivos .DAT. Para usar esta função, você deve ter configurado a maioria das opções necessárias para que o AutoUpdate localize o site da lista e, se for necessário, estabeleça a conexão. Veja "Configurando as opções de atualização" na página 223 para saber como especificar as opções necessárias.

  Se o AutoUpdate não puder conectar-se ao site da lista após três tentativas, ou se não encontrar novos arquivos .DAT, ele estabelecerá a conexão com cada um dos outros sites da lista até encontrar os arquivos .DAT mais atuais disponíveis. Se você tiver selecionado a opção **Forçar Atualização**, o AutoUpdate fará download de quaisquer arquivos .DAT que encontrar no primeiro site com o qual possa conectar-se com sucesso. Veja "Configurando opções de atualização avançadas" na página 226 para obter mais detalhes.

2. Clique na guia Atividade de Registro para exibir a próxima página de propriedades (Figura 6-19).
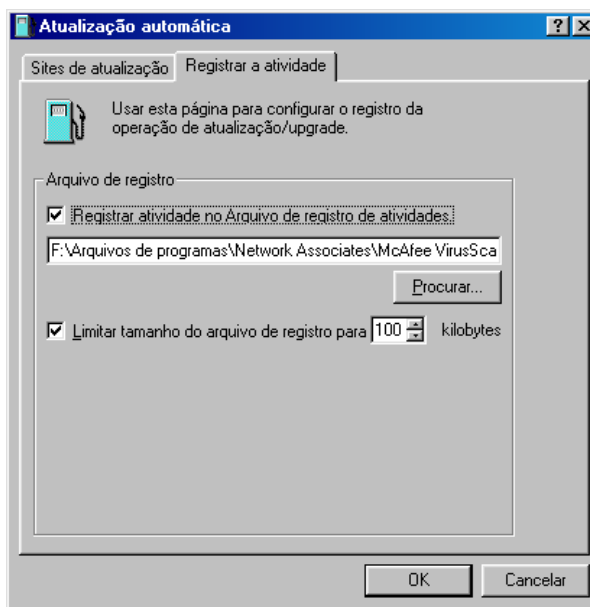
Figura 6-19. Caixa de diálogo Atualização Automática - página Atividade de registro

3. Marque a caixa de verificação **Registrar atividade no Arquivo de registro de atividades**.

   Como padrão, o AutoUpdate registra o que acontece durante tentativas de atualização e salva o registro no arquivo UPDATE UPGRADE ACTIVITY LOG.TXT no diretório de programa do VirusScan. Você pode digitar um nome e um caminho diferentes na caixa de texto mostrada, ou clicar em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

4. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada

   Digite um valor entre 10Kb e 999Kb. Como padrão, o AutoUpdate limita o tamanho do arquivo a 100KB. Se os dados no registro ocuparem mais espaço que o tamanho do arquivo que você definiu, o AutoUpdate apagará o registro existente e recomeçará do ponto onde foi interrompido. Para ver o conteúdo do arquivo de registro no Programador de Tarefas do VirusScan, selecione a tarefa AutoUpdate na lista de tarefas, em seguida escolha **Exibir Registro de Atividades** no menu **Tarefa**.

5. Clique em **OK** para salvar as suas alterações e fechar a caixa de diálogo Atualização Automática. Clique em **Cancelar** para fechar a caixa de diálogo sem salvar as alterações. O AutoUpdate salva todas as alterações feitas na caixa de diálogo Atualização Automática no UPDATE.INI, um arquivo armazenado no diretório de programa do VirusScan. Para replicar essas configurações em toda a sua rede, copie o UPDATE.INI para o diretório de programa do VirusScan em cada nó de rede.

Configurando as opções de atualização

Para criar um novo site de atualização ou alterar as configurações de um site existente, clique em **Adicionar** na caixa de diálogo Atualização automática (veja Figura 6-17 na página 220) ou selecione um site na lista, em seguida clique em **Editar**. Ambos os procedimentos abrirão a caixa de diálogo Propriedades da atualização automática (Figura 6-20 na página 224).
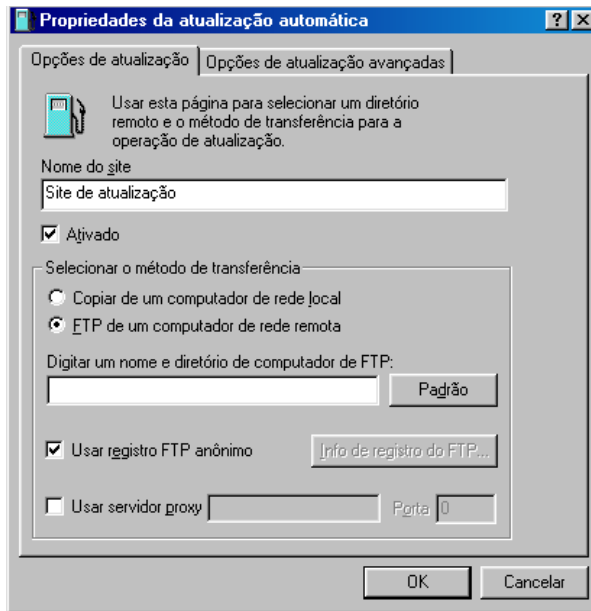
Figura 6-20. Caixa de diálogo Propriedades da atualização automática. - página Opções de atualização

Depois, siga estas etapas:

1. Digite um nome para o site na caixa de texto mostrada. Escolha um nome descritivo que você reconhecerá na lista de sites.

2. Clique em **Ativado** para informar ao AutoUpdate que se conecte a este site no horário programado. Desmarcar essa caixa de verificação preserva as opções que você configurou, mas informa ao AutoUpdate que não verifique este site.

   O AutoUpdate fará no máximo três tentativas de conexão a este site durante cada operação de atualização planejada. Quando conecta-se e faz download do novo pacote de arquivos .DAT, o AutoUpdate também extrai os arquivos e instala-os no diretório de programa do VirusScan.

3. Escolha o método que você deseja utilizar para conectar-se ao servidor de destino. Estas são as opções:

- **Copiar de um computador de rede local**. Selecione esta opção para transferir apenas os arquivos de atualização de um computador da rede através de qualquer protocolo de rede comum que esteja ativado. As definições para este protocolo controlam o modo como o AutoUpdate tenta estabelecer a conexão e o período do tempo de espera que deve transcorrer antes que o AutoUpdate pare a tentativa de conexão.

  Digite o nome do computador usando a notação Universal Naming Convention (UNC) na caixa de texto mostrada ou clique em **Procurar** para localizar o computador na rede. As opções restantes na caixa de diálogo são desativadas.

- **FTP de um computador de rede remota**. Selecione esta opção para transferir os arquivos de atualização via File Transfer Protocol (FTP). Para usar essa opção, o servidor de destino deve ter um serviço de FTP ativado.

  O AutoUpdate utiliza o seu próprio FTP para conectar-se ao servidor, o período de tempo de espera para a tentativa de conexão dependerá das definições de protocolo rede existentes.

  Em seguida, digite o nome do domínio para servidor de destino, junto com qualquer outra informação necessária sobre o diretório, na caixa de texto mostrada. O clique em **Padrão** define o servidor FTP da Network Associates.

  Se o servidor de destino aceitar conexões de FTP anônimas, marque a caixa de diálogo **Usar conexão de FTP anônima**. Se você usar uma conta de FTP específica que necessite de um nome de usuário e de uma senha, desmarque a caixa de seleção, em seguida clique em **Informação de conexão de FTP**. Esse botão abre uma caixa de diálogo na qual você pode digitar o nome de usuário e a senha correta. Repita a senha para confirmá-la, em seguida **OK** para fechar a caixa de diálogo.

4. Se você rotear as solicitações de FTP da sua rede através de um servidor proxy, marque a caixa de verificação **Usar servidor proxy**, em seguida digite o nome do seu servidor proxy na caixa de texto mostrada. É possível especificar o nome usando a notação UNC ou como um nome de domínio, o que for mais apropriado para o seu ambiente. Em seguida, na caixa de texto restante, digite a porta lógica para o servidor proxy ao qual o AutoUpdate deve enviar a sua solicitação de FTP.

5. Para escolher opções adicionais, clique na guia Atualização Avançada. Para salvar as alterações e retornar à caixa de diálogo Atualização Automática, clique em **OK**. O AutoUpdate salva todas as suas alterações feitas na caixa de diálogo Atualização Automática no UPDATE.INI, um arquivo armazenado no diretório de programa do VirusScan. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

Configurando opções de atualização avançadas

Para completar a sua tarefa AutoUpdate, você precisa digitar apenas um servidor de destino, um método de conexão e qualquer informação necessária sobre conexão. Em seguida, quando a tarefa tiver sido ativada e um planejamento definido para ela, o AutoUpdate fará download dos arquivos corretos no servidor de destino para você, descompacte os arquivos .ZIP e instale-os no diretório de programa do VirusScan.

Para que o AutoUpdate faça um processamento adicional, anterior ou posterior, dos arquivos ou realize outras ações, clique na guia Opções de Atualização Avançadas para exibir a página de propriedades correta (Figura 6-21).
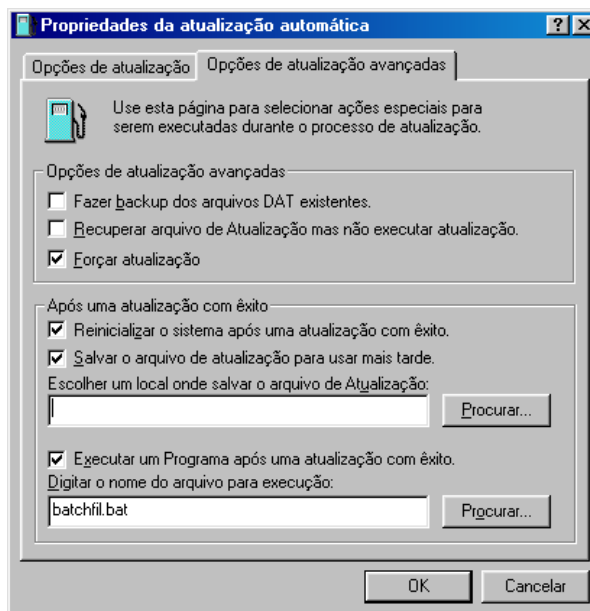
Figura 6-21. Caixa de diálogo Propriedades da atualização automática - página Opções de atualização avançadas

Depois, siga estas etapas:

1. Informe ao AutoUpdate o que deve fazer antes ou durante uma atualização. Estas são as opções:

   - **Backup dos arquivos .DAT existentes.** Marque essa caixa de verificação para que o AutoUpdate renomeie os arquivos .DAT do VirusScan existentes antes de instalar os novos. Para renomear cada arquivo, o AutoUpdate anexa a extensão .SAV no nome de arquivo e na extensão existentes. CLEAN.DAT, por exemplo, será renomeado como CLEAN.DAT.SAV.

   - **Recuperar arquivo de Atualização sem instalar**. Marque esta caixa de verificação para que o AutoUpdate faça download do arquivo .ZIP que contém os novos arquivos .DAT e apenas salve-o em uma localização que você especificou em vez de descompactar e instalá-lo.

     A marcação dessa caixa de verificação também define **Salvar o arquivo de Atualização para uso posterior** para a área **Após atualização bem-sucedida**. Para informar ao AutoUpdate onde deve salvar o pacote de arquivos .DAT, digite um caminho e um nome de pasta na caixa de texto abaixo dessa caixa de verificação, ou clique em **Procurar** para localizar uma pasta adequada.

     Esta opção pode ser conveniente se você quiser fazer download dos novos arquivos .DAT para um servidor central na sua rede e que os computadores de clientes individuais também façam download, descompactem e instalem os novos arquivos localmente.

   - **Forçar Atualização.** Marque esta caixa de verificação para informar ao AutoUpdate que faça download e instale qualquer pacote de arquivos .DAT que encontrar no servidor de destino, sendo ou não o pacote mais recente que os seus arquivos .DAT existentes. Você pode usar essa opção para “renovar” periodicamente arquivos .DAT armazenados no diretório de programa do VirusScan, no caso de seus arquivos existentes terem sido danificados. Essa opção também contornará qualquer mensagem de erro que o VirusScan possa retornar se ele não encontrar novos arquivos no servidor de destino na hora planejada para a tarefa de atualização.

ATENÇÃO: A Network Associates recomenda a utilização desta opção com extrema cautela. Se a sua tarefa AutoUpdate estiver configurada para estabelecer conexão com um servidor que armazene versões mais antigas de arquivos .DAT, você poderá reduzir a eficácia do VirusScan e expor o seu computador e a rede a infecções por novos vírus e outros softwares destrutivos. As atualizações de versão dos componentes de programa do VirusScan também podem causar incompatibilidades com versões mais antigas de arquivos .DAT. Essas incompatibilidades podem, por sua vez, fazer com que o VirusScan comporte-se de maneira imprevisível.

2. Para informar ao AutoUpdate que, após downloads bem-sucedidos, deve extrair e instalar os novos arquivos .DAT. Estas são as opções:

   - **Reinicializar o sistema, se necessário, após uma atualização bem-sucedida**. Marque esta caixa de verificação para que o AutoUpdate reinicie o seu sistema após instalar os novos arquivos .DAT.

     Embora o VirusScan e o VShield necessitem que você reinicie o sistema para carregar os novos arquivos .DAT, é possível que você queira fazê-lo apenas durante as horas de inatividade para não interferir na produção. Se você planeja executar um programa após atualizar os arquivos .DAT, deverá deixar essa caixa de verificação desmarcada.

     NOTA: Essa opção funciona apenas para operações de atualização planejadas. Ao clicar em **Atualizar Agora** na caixa de diálogo Atualização Automática, o AutoUpdate lhe perguntará se deseja reiniciar o computador assim que terminar a instalação dos novos arquivos .DAT , estando ou não essa opção selecionada.

- **Salvar o arquivo de Atualização para uso posterior.** Marque esta caixa de verificação para que o AutoUpdate salve uma cópia compactada do pacote de arquivos .DAT na localização especificada. O AutoUpdate, em seguida, extrai os arquivos .DAT do pacote de atualização e continua a instalação. Ao contrário, a opção **Recuperar arquivo de Atualização sem instalar** salva o arquivo compactado, mas não instala os novos arquivos .DAT.

  Para informar ao AutoUpdate onde salvar o pacote de arquivos .DAT, digite um caminho e o nome de uma pasta na caixa de texto abaixo desta caixa de verificação ou clique em **Procurar** para localizar uma subpasta adequada.

- **Executar um programa após Atualização bem-sucedida.** Marque esta caixa de verificação para informar ao AutoUpdate que inicie outro programa após terminar de instalar os novos arquivos .DAT. Essa opção pode ser utilizada, por exemplo, para iniciar um programa de cliente de correio eletrônico ou um utilitário de mensagem de rede que notifica um administrador sobre a conclusão bem-sucedida da operação.

  Em seguida, digite o caminho e o nome de arquivo do programa que você deseja executar ou clique em **Procurar** para localizar o programa no seu disco rígido.

3. Para salvar as suas alterações e retornar à caixa de diálogo Atualização Automática, clique em **OK**. O AutoUpdate salva todas as alterações feitas na caixa de diálogo Atualização Automática no UPDATE.INI, um arquivo armazenado no diretório de programa do VirusScan. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

Configurando as opções do AutoUpgrade

A Network Associates revisa o VirusScan freqüentemente para adicionar novos recursos de detecção e reparo, novas funcionalidade para uma melhor administração e flexibilidade, além de outros aprimoramentos que o tornam a melhor ferramenta de segurança antivírus. O utilitário AutoUpgrade do VirusScan é projetado especificamente para procurar e fazer download dessas novas versões quando tornam-se disponíveis.

NOTA: "Atualizar" o VirusScan significa fazer download e instalar novas versões dos arquivos .DAT; "atualizar a versão" do VirusScan significa fazer download e instalar revisões da versão do produto, de executáveis e, em alguns casos, de arquivos .DAT. A Network Associates oferece atualizações gratuitas dos arquivos .DAT de dados durante a vida do produto. Porém, isso não garante que esses arquivos serão compatíveis com as versões anteriores do produto.

O seu direito de fazer download grátis de atualizações de versão do VirusScan depende dos termos da sua licença ou do contrato de venda com o qual você concordou no momento da compra do produto. Se você tiver perguntas a fazer sobre esses termos, consulte os documentos LICENSE.TXT ou README.1ST incluídos na sua cópia do VirusScan ou entre em contato com o seu representante de vendas. A Network Associates torna disponíveis os arquivos de atualização de versão para download grátis nos sites de FTP e outros serviços contanto que a sua licença permita. O Programador de Tarefas do VirusScan usa uma tarefa diferente, o AutoUpgrade, para controlar quando e com que freqüência devem ser obtidos por download os novos arquivos do VirusScan. Veja "Configurando as opções do AutoUpgrade" na página 230 para saber como configurar essa tarefa.

Como padrão, a tarefa AutoUpgrade incluída no Programador de Tarefas do VirusScan não está configurada com as informações sobre o site necessárias para fazer download das novas versões do VirusScan. Os usuários do VirusScan registrados podem obtê-las de seus representantes de vendas ou da Network Associates.

A Network Associates recomenda o uso do AutoUpdate junto com o serviço complementar, Enterprise SecureCast, numa estrutura "push-pull" eficiente. Uma vez instalado o seu software de cliente em um servidor administrativo, o SecureCast pode enviar, ou "push", os arquivos atualizados para você automaticamente, assim que a McAfee Labs os tornar disponíveis. Veja "Configurando o Enterprise SecureCast" na página 283 para obter mais detalhes.

Se você tornar disponíveis esses arquivos atualizados em um ou mais servidores centrais na sua rede e configurar os nós de rede restantes para receber, “pull”, os arquivos atualizados desses servidores, poderá

- Planejar um revezamento de distribuições em toda a rede de novas versões do VirusScan para horários convenientes e com uma mínima intervenção de administradores ou usuários de rede. Com a caixa de diálogo Propriedades da tarefa do Programador de Tarefas do VirusScan, é possível determinar quando cada nó de rede fará consulta seqüencial para procurar arquivos atualizados.

  Você pode, por exemplo, especificar um horário de atualização conveniente para executar o AutoUpgrade quando distribuir o VirusScan pela primeira vez, mas defina-o para ser acionado em um intervalo aleatório dentro de 60 minutes a partir da hora especificada, ou defina um planejamento periódico ou rotativo entre diferentes partes da rede. Para saber como planejar o AutoUpgrade ou outras tarefas, veja “Ativando tarefas” na página 192.

- Reparta os serviços de administração periódica entre os diversos servidores e controladores de domínio, entre diferentes áreas das redes remotas ou por todas as outras divisões da rede. A manutenção do tráfego de atualização basicamente interno também pode reduzir as quebras de segurança de rede potenciais.

- Reduzir a probabilidade do tempo de espera necessário para fazer download de novas versões do VirusScan. O tráfego nos servidores da. Network Associates aumenta significativamente quando novas versões do VirusScan são lançadas. Evitar a competição por larguras de banda na rede lhe possibilita distribuir novas versões com interrupções mínimas.

IMPORTANTE: Se você armazenar os novos arquivos de atualização de versão do VirusScan em um servidor sensível a maiúsculas e minúsculas em nomes de arquivos, deverá renomear o PKGDESC.INI, arquivo que acompanha as atualizações de versão do VirusScan, para que ele use apenas letras minúsculas. Caso contrário, o AutoUpgrade não encontrará o arquivo no servidor e não instalará a nova versão do VirusScan nos computadores de clientes.

Outras opções avançadas do AutoUpgrade permitem reinicializar o sistema ou salvar o pacote de atualização de versão para ser utilizado posteriormente. Um conjunto de páginas de propriedades do AutoUpgrade controla as opções para essa tarefa — clique em cada guia na caixa de diálogo Propriedades da atualização de versão automática para configurá-las.

Para configurar o AutoUpgrade, siga estas etapas:

1. Selecione a tarefa AutoUpgrade mostrada na janela do Programador de Tarefas, em seguida em [ícone] na barra de ferramentas do Programador de Tarefas.

NOTA: O AutoUpgrade é executado de acordo com o planejamento definido na caixa de diálogo Propriedades da tarefa. Uma alternativa para abrir essa caixa de diálogo é selecionar a tarefa AutoUpgrade, em seguida clicar [ícone] na barra de ferramentas do Programador de tarefas. Para saber mais sobre a maneira de definir um planejamento de tarefa, veja “Ativando tarefas” na página 192.

A caixa de diálogo Atualização de versão automática aparecerá (veja Figura 6-22).
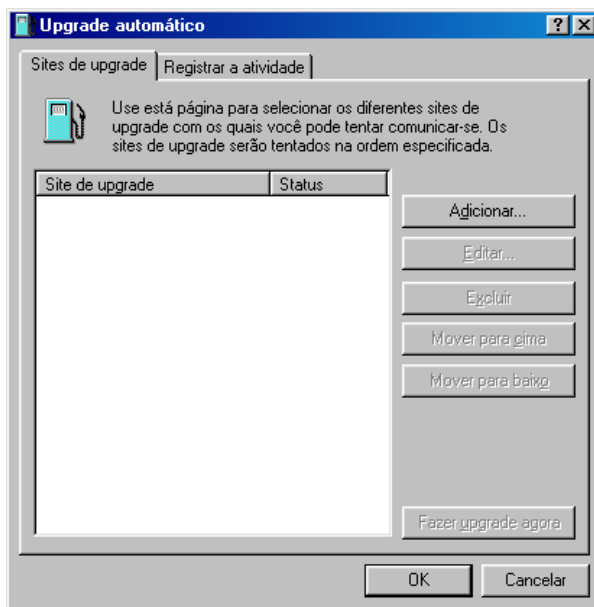
Figura 6-22. Caixa de diálogo Atualização de versão automática - página Sites de atualização de versão

Nessa etapa, o AutoUpgrade faz uma lista dos sites nos quais fará download dos novos arquivos .DAT. Inicialmente, você não verá nenhum site na lista porque o AutoUpgrade não está configurado para conectar-se a qualquer site de atualização de versão. Os sites necessários devem ser adicionados a partir das informações recebidas ao comprar o VirusScan. É possível adicionar quantos sites diferentes você quiser e alterar a ordem na qual o AutoUpgrade tenta estabelecer essas conexões a partir dessa caixa de diálogo. Estas são as opções:

- **Adicionar um novo site.** Clique em **Adicionar** para abrir a caixa de diálogo Propriedades da atualização de versão automática (Figura 6-23). Para saber como especificar opções para o novo site, veja "Configurando as opções de atualização" na página 235.
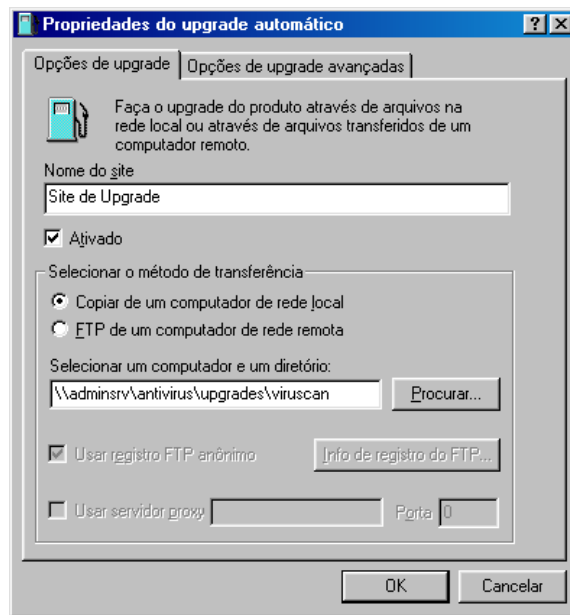
Figura 6-23. Caixa de diálogo Propriedades da atualização de versão automática-página Opções de atualização de versão

- **Alterar as opções para um site existente.** Selecione um dos sites mostrados na lista, em seguida clique em **Editar** para abrir a caixa de diálogo Propriedades da atualização de versão automática (veja Figura 6-23). Faça as alterações que você quiser, em seguida clique em **OK** para fechar a caixa de diálogo. Para ver as descrições e instruções a fim de configurar as opções disponíveis, veja "Configurando as opções de atualização" na página 235.

- **Remover um site existente.** Selecione um dos sites mostrados na lista, em seguida clique em **Excluir** para removê-lo.

- **Alterar a ordem de pesquisa nos sites existentes.** Para alterar a ordem na qual o AutoUpgrade conecta-se aos sites da lista na caixa de diálogo, selecione o site cuja prioridade você deseja alterar, em seguida clique em **Mover para cima** para dar ao site uma prioridade mais alta, ou **Mover para baixo** para dar ao site uma prioridade mais baixa.

- **Atualizar a versão de seus arquivos VirusScan imediatamente.** Clique em **Atualizar a versão agora** para que o AutoUpgrade conecte-se imediatamente ao primeiro site da lista e procure uma nova versão do VirusScan. Para usar esta função, você deve ter configurado a maioria das opções necessárias para que o AutoUpgrade localize o site da lista e, se for necessário, estabeleça a conexão. Veja "Configurando as opções de atualização" na página 235 para saber como especificar as opções necessárias.

  Se o AutoUpgrade não puder conectar-se ao site da lista após três tentativas ou se não encontrar novos arquivos do VirusScan ele estabelecerá a conexão com cada um dos outros sites da lista até encontrar os arquivos mais atualizados da versão do VirusScan disponíveis.

2. Clique na guia Atividade de registro para exibir a próxima página de propriedades (Figura 6-24).
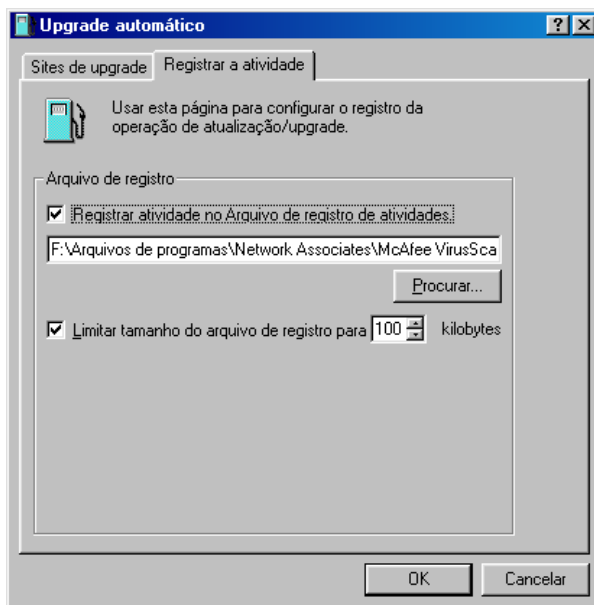
Figura 6-24. Caixa de diálogo Atualização de versão automática - página Atividade de registro

3. Marque a caixa de verificação **Registrar atividade no Arquivo de registro de atividades**.

   Como padrão, o AutoUpgrade grava o que acontece durante as tentativas de atualização e salva o registro no arquivo UPDATE UPGRADE ACTIVITY LOG.TXT no diretório de programa do VirusScan. Você pode digitar um nome e um caminho diferentes na caixa de texto mostrada, ou clicar em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

4. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada.

   Digite um valor entre 10Kb e 999Kb. Como padrão, o AutoUpgrade limita o tamanho do arquivo a 100KB. Se os dados no registro ocuparem mais espaço que o tamanho do arquivo que você definiu, o AutoUpgrade apagará o registro existente e recomeçará do ponto onde foi interrompido. Para ver o conteúdo do arquivo de registro no Programador de Tarefas do VirusScan, selecione a tarefa AutoUpgrade na lista de tarefas, em seguida escolha **Exibir registro de atividades** no menu **Tarefa**.

5. Clique em **OK** para salvar as suas alterações e fechar a caixa de diálogo Atualização de versão automática. Clique em **Cancelar** para fechar a caixa de diálogo sem salvar as alterações. O AutoUpgrade salva todas as alterações feitas na caixa de diálogo Atualização de versão automática no UPGRADE.INI, um arquivo armazenado no diretório de programa do VirusScan. Para replicar essas configurações em toda a sua rede, copie o UPGRADE.INI para o diretório de programa do VirusScan em cada nó de rede.

Configurando as opções de atualização

Para criar um novo site de atualização de versão ou alterar as configurações de um site existente, clique em **Adicionar** na caixa de diálogo Atualização de versão automática (veja Figura 6-22 na página 232) ou selecione um site na lista, em seguida clique em **Editar**. Ambos os procedimentos abrirão a caixa de diálogo Propriedades da atualização de versão automática (Figura 6-25 na página 236).
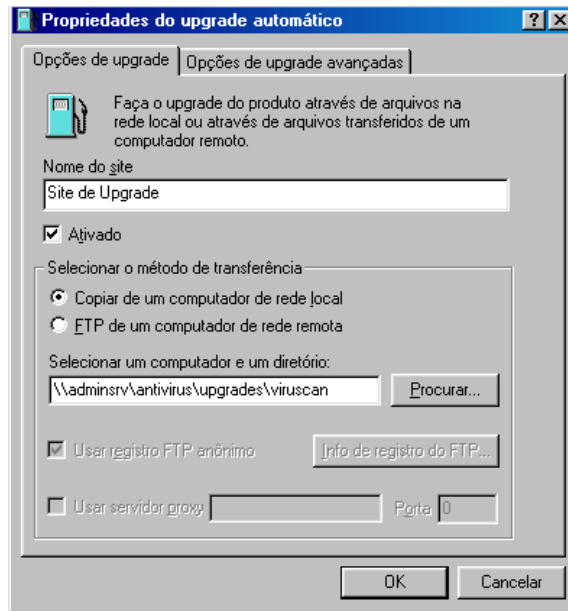
Figura 6-25. Caixa de diálogo Propriedades da atualização de versão automática - página Opções de atualização de versão

---

Depois, siga estas etapas:

1. Digite um nome para o site na caixa de texto mostrada. Escolha um nome descritivo que você reconhecerá na lista de sites.

2. Clique em **Ativado** para informar ao AutoUpgrade que se conecte a este site no horário programado. Desmarcar essa caixa de verificação preserva as opções que você configurou, mas instrui o AutoUpgrade a não verificar este site.

   O AutoUpgrade fará no máximo três tentativas de conexão a este site durante cada operação de atualização planejada. Quando se conecta e faz download de uma nova versão do VirusScan, o AutoUpgrade também extrai os arquivos e instala-os no diretório de programa do VirusScan.

3. Escolha o método que você deseja utilizar para conectar-se ao servidor de destino. Estas são as opções:

- **Copiar de um computador de rede local**. Selecione esta opção para transferir apenas os arquivos de atualização de um computador da rede através de qualquer protocolo de rede comum que esteja ativado. As definições para este protocolo controlam o modo como o AutoUpgrade tenta estabelecer a conexão e o período do tempo de espera que deve transcorrer antes que pare de tentar a conexão.

  Digite o nome do computador usando a notação Universal Naming Convention (UNC) na caixa de texto mostrada ou clique em **Procurar** para localizar o computador na rede. As opções restantes na caixa de diálogo são desativadas.

- **FTP de um computador de rede remota**. Selecione esta opção para transferir os arquivos de atualização via File Transfer Protocol (FTP). Para usar essa opção, o servidor de destino deve ter um serviço de FTP ativado.

  O AutoUpgrade utiliza o seu próprio FTP para conectar-se ao servidor, mas o período de tempo de espera para a tentativa de conexão dependerá das definições de protocolo rede existentes.

  Em seguida, digite o nome do domínio para servidor de destino, junto com qualquer outra informação necessária sobre o diretório, na caixa de texto mostrada, ou clique em **Procurar** para localizar o servidor na rede.

  Se o servidor de destino aceitar conexões de FTP anônimas, marque a caixa de verificação **Usar conexão de FTP anônima**. Se você usar uma conta de FTP específica que necessite de um nome de usuário e de uma senha, desmarque a caixa de verificação, em seguida clique em **Informação de conexão de FTP**. Esse botão abre uma caixa de diálogo na qual você pode digitar o nome de usuário e a senha correta. Repita a senha para confirmá-la, em seguida **OK** para fechar a caixa de diálogo.

4. Se você rotear as solicitações de FTP da sua rede através de um servidor proxy, marque a caixa de verificação **Usar servidor proxy** em seguida digite o nome do seu servidor proxy na caixa de texto mostrada. É possível especificar o nome usando a notação UNC ou como um nome de domínio, o que for mais apropriado para o seu ambiente. Em seguida, na caixa de texto restante, digite a porta lógica para o servidor proxy ao qual o AutoUpgrade deve enviar a sua solicitação de FTP.

5. Para escolher opções adicionais, clique na guia Atualização de Versão Avançada. Para escolher opções adicionais, clique na guia Atualização de Versão Avançada **OK**. O AutoUpgrade salva todas as suas alterações feitas na caixa de diálogo Atualização de versão automática no UPGRADE.INI, um arquivo armazenado no diretório de programa do VirusScan. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

Configurando opções de atualização de versão avançadas

Para completar a sua tarefa AutoUpgrade você precisa digitar apenas um servidor de destino, um método de conexão e qualquer informação necessária sobre conexão. Em seguida, quando a tarefa tiver sido ativada e um planejamento definido para ela, o AutoUpgrade fará download dos arquivos corretos no servidor de destino para você, descompactará os arquivos .ZIP e os instalará no diretório de programa do VirusScan.

Para que o AutoUpgrade atue de outras formas antes ou depois de localizar os novos arquivos, clique na guia Opções de Atualização de versão avançadas para exibir a página de propriedades correta (Figura 6-26).
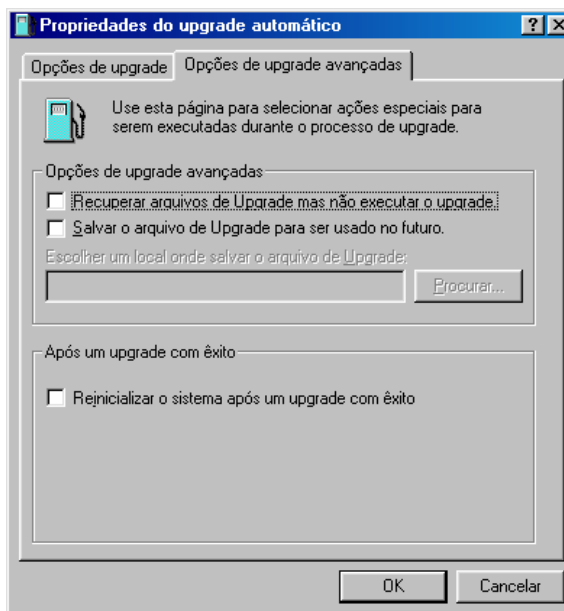
Figura 6-26. Caixa de diálogo Propriedades da atualização de versão automática - página Opções de atualização de versão avançadas

Depois, siga estas etapas:

1. Informe ao AutoUpgrade o que deve fazer com os arquivos dos quais fez download. Estas são as opções:

   - **Recuperar arquivos de Atualização de Versão sem instalar**. Marque esta caixa de verificação para que o AutoUpgrade faça download da nova versão do VirusScan e apenas salve-o em uma localização que você especificou em vez de descompactar e instalá-lo.

     A marcação dessa caixa de verificação também define **Salvar o arquivo de Atualização de Versão para uso posterior** . Para informar ao AutoUpgrade onde deve salvar os novos arquivos, digite um caminho e um nome de pasta na caixa de texto abaixo dessa caixa de verificação, ou clique em **Procurar** para localizar uma pasta adequada.

     Esta opção pode ser conveniente se você quiser fazer download dos novos arquivos do VirusScan para um servidor central na sua rede e que os computadores de clientes individuais também descarreguem, descompactem e instalem os novos arquivos localmente.

   - **Salvar arquivos de Atualização de Versão para uso posterior.** Marque essa caixa de verificação para que o AutoUpgrade salve uma cópia compactada dos novos arquivos do VirusScan em um local especificado. O AutoUpgrade continua, em seguida, a instalação. Por outro lado, a opção **Recuperar arquivos de Atualização sem instalar** salva o arquivo compactado, mas não instala a nova versão do VirusScan.

2. Para informar ao AutoUpgrade que, após downloads bem-sucedidos, deve extrair e instalar uma nova versão do VirusScan, estas são as opções:

   - **Reinicializar o sistema, se necessário, após uma atualização de versão bem-sucedida**. Marque esta caixa de verificação para que o AutoUpgrade reinicie o seu sistema após instalar os novos arquivos do VirusScan.

     Embora o VirusScan e o VShield necessitem que você reinicie o sistema após a instalação, é possível que você queira fazê-lo apenas durante as horas de inatividade para não interferir na produção.

NOTA: Esta opção funciona apenas para operações de atualização versão planejadas. Ao clicar em **Atualizar versão agora** na caixa de diálogo Atualização de versão automática, o AutoUpgrade lhe perguntará se deseja reiniciar o computador assim que terminar a instalação da versão do VirusScan, estando ou não essa opção selecionada.

3. Para salvar as suas alterações e retornar à caixa de diálogo Atualização de versão automática, clique em **OK**. O AutoUpgrade salva todas as modificações na caixa de diálogo Atualização de versão automática no UPGRADE.INI, um arquivo armazenado no diretório de programa do VirusScan. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

Configurando opções para outros programas

Você pode usar o Programador de Tarefas para executar outros programas em momentos específicos, porém a menos que o programa seja um produto antivírus da Network Associates, não é possível usar o Programador de Tarefas para configurá-lo, de modo a utilizar determinadas opções. Para fazer isso, o programa deve ser aberto e pré-configurado — o Programador de Tarefas executará apenas o programa como foi configurado, no momento especificado. Contudo, você pode usar o Programador de Tarefas para abrir a caixa de diálogo Propriedades do VShield a fim de configurá-lo para que use opções específicas em sua execução. Para saber como fazê-lo, veja o Capítulo 4, “Usando o VShield.”

Usando ferramentas de varredura Especializadas

7

Varredura de correio do Microsoft Exchange e Outlook

Além da varredura contínua, em segundo plano, que o VShield lhe fornece através do seu módulo Varredura de Correio Eletrônico, o VirusScan inclui um componente de programa com recursos completos, projetado especificamente para procurar vírus nas suas caixas de correio do Microsoft Exchange e Microsoft Outlook, ou em qualquer servidor de correio que funcione com a Messaging Application Programming Interface (MAPI) da Microsoft. O componente de programa Varredura de Correio Eletrônico possibilita o exame dos servidores de correio, quando o usuário quiser e lhe for mais conveniente. Uma arquitetura de plug-ins discreta dá acesso ao scanner diretamente a partir do aplicativo de cliente Exchange ou Outlook.

Se você tiver escolhido a opção de instalação Típica para o VirusScan (veja página 42 para obter mais detalhes), já terá acesso ao componente de programa Varredura de Correio Eletrônico.

Para usar o componente de programa Varredura de Correio Eletrônico com as suas configurações padrão, basta iniciar o software de cliente Microsoft Exchange ou Microsoft Outlook e em seguida

1. Conectar-se ao seu servidor de correio eletrônico normalmente.
2. Escolha **Examinar vírus** no menu **Ferramentas** ou clique em na barra de ferramentas do Exchange ou Outlook.

> **NOTA:** Se você usar o Microsoft Exchange 5.0, uma limitação no modo com que o programa atualiza a barra de ferramentas impede que a Varredura de Correio Eletrônico exiba os seus botões imediatamente. Para adicionar o botão Examinar vírus na barra de ferramentas, escolha **Personalizar barra de ferramentas** no menu **Ferramentas**, em seguida, acrescente os botões da Varredura de Correio Eletrônico, da lista de botões disponíveis, na caixa de diálogo Personalizar barra de ferramentas.

Uma vez iniciada, a Varredura de Correio Eletrônico começará imediatamente a examinar as caixas de correio do Exchange ou Outlook (veja Figura 7-1).

Como padrão, a Varredura de Correio Eletrônico examina *todas* as suas mensagens de correio eletrônico armazenadas na Caixa de entrada do servidor de correio, para procurar anexos suscetíveis a infecção por vírus. Se você tiver muitas mensagens armazenadas no servidor, que ainda não foram descarregadas, essa operação de varredura pode demorar bastante. Para fazer uma pausa na operação, clique em . Se quiser parar a varredura, clique em . Para continuar a operação, clique em .
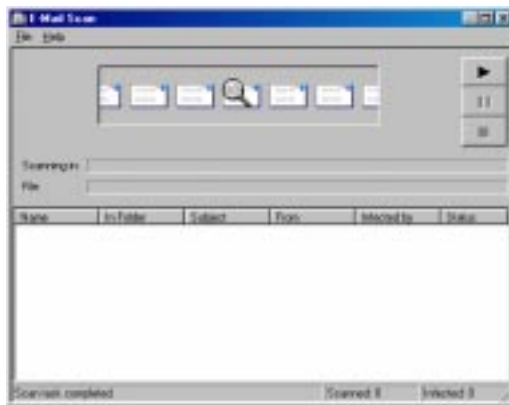
Figura 7-1. Varredura de Correio Eletrônico em andamento

Se encontrar um arquivo infectado, a Varredura de Correio Eletrônico lhe solicitará uma ação contra o vírus. Veja “Reagindo quando a Varredura de Correio Eletrônico detecta um vírus” na página 76 para obter mais detalhes.

Configurando o componente de programa Varredura de Correio Eletrônico

Embora as configurações padrão da Varredura de Correio Eletrônico lhe dêem uma boa proteção contra infecções transmitidas através do correio eletrônico do Exchange ou Outlook, poderão não ser adequadas aos seus hábitos de trabalho.

Para modificar as opções de configuração da Varredura de Correio Eletrônico, siga estas etapas:

1. Inicie o software de cliente Exchange ou Outlook, em seguida, conecte-se ao servidor de correio eletrônico.

   NOTA: Caso você já esteja conectado ao domínio da rede que hospeda o servidor de correio eletrônico, não precisará conectar-se ao seu servidor diretamente — em vez disso, inicie o Exchange ou Outlook. Entre em contato com o seu administrador de rede para saber quais são os requisitos de conexão do servidor.

2. Escolha **Propriedades da Varredura de Correio Eletrônico** no menu **Ferramentas** em qualquer um dos programas ou clique em , na barra de ferramentas do Exchange ou Outlook.

   Aparece a caixa de diálogo Propriedades da Varredura de Correio Eletrônico (veja a Figura 7-2). A caixa de diálogo Propriedades consiste de páginas de propriedades que controlam as definições da Varredura de Correio Eletrônico — clique em cada guia para configurar o programa de acordo com as suas necessidades.

Figura 7-2. Caixa de diálogo Varredura de Correio Eletrônico – página Detecção

Escolhendo opções de Detecção

A Varredura de Correio Eletrônico assume inicialmente que você quer examinar todas as mensagens de correio eletrônico armazenadas no servidor do Exchange ou Outlook, e restringir os arquivos examinados somente aos suscetíveis a infecção por vírus (veja Figura 7-2 na página 243).

Para alterar essas configurações, siga estas etapas:

1. Informe à Varredura de Correio Eletrônico quais mensagens de correio eletrônico devem ser examinada. Estas são as opções:

   - **Todas as mensagens.** Selecione esse botão para que a Varredura de Correio Eletrônico examine todas as mensagens armazenadas, no momento, no servidor do Exchange. Esta varredura, por ser abrangente, pode demorar muito.

   - **Somente mensagens não lidas.** Selecione este botão para que a Varredura de Correio Eletrônico examine somente as mensagens marcadas com "não foi lida." Após a varredura da caixa de correio inteira, escolha esta opção para acelerar as operações de varredura, mantendo uma proteção antivírus completa para o seu computador.

   NOTA: Quando você tiver feito download do correio para o computador, o VirusScan trata a sua pasta pessoal ou o arquivo de armazenamento como qualquer outro, a menos que seja especificamente excluído das operações de varredura. Isto lhe fornece uma segurança antivírus reforçada.

2. Informe à Varredura de Correio Eletrônico quais tipos de anexos devem ser examinados. Você pode

   - **Examinar arquivos compactados.** Marque a caixa de verificação **Arquivos compactados** para que a Varredura de Correio Eletrônico procure vírus em arquivos compactados com estes formatos: .??_, .CAB, LZEXE, LZH, PKLite, .TD0 e .ZIP. Embora proporcione melhor proteção, a varredura de arquivos compactados pode tornar mais lenta uma operação de varredura.

- **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Contudo, você pode reduzir a abrangência das operações de varredura para que a Varredura de Correio Eletrônico examine apenas os anexos mais suscetíveis a infecções por vírus. Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou determinar as extensões de nomes de arquivos que a Varredura de Correio Eletrônico examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (Figura 7-3).
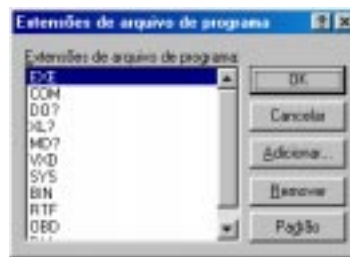
Figura 7-3. Caixa de diálogo Extensões de arquivo de programa

Caixa de diálogo Extensões de arquivo de programa Como padrão, a Varredura de Correio Eletrônico procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD e .DLL. Os arquivos com as extensões .DO?, .XL?, .RTF e .OBD pertencem ao Microsoft Office e podem ser infectados por vírus de macros. O ? é um curinga que ativa Varredura de Correio Eletrônico para examinar arquivos de documentos e de modelos.

– Para adicionar uma extensão a lista, clique em **Adicionar**, em seguida, digite as extensões que o VirusScan deverá examinar na caixa de diálogo mostrada.

– Para remover uma extensão da lista, selecione-a, em seguida, clique em **Remover**.

– Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

Para que a Varredura de Correio Eletrônico examine todos os arquivos do seu sistema, com qualquer extensão, selecione o botão **Varredura de todos os anexos de arquivos**. Embora este procedimento ofereça mais proteção, tornará as operações de varredura consideravelmente mais lentas.

- **Ativar a varredura heurística**. Clique em **Heuristics** para abrir a caixa de diálogo Configurações da varredura heurística (Figura 7-4).
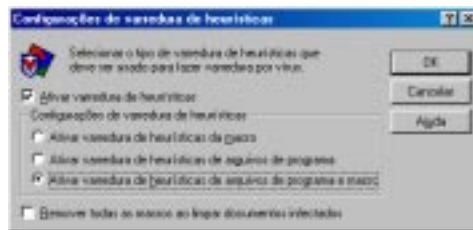
Figura 7-4. Caixa de diálogo Configurações da varredura heurística

A tecnologia da varredura heurística possibilita à Varredura de Correio Eletrônico reconhecer novos vírus com base na sua semelhança com vírus que o VirusScan já conhece. Para fazê-lo, o programa procura determinadas características "semelhantes a vírus" nos arquivos que você pediu para serem examinados. A presença de um número suficiente desses elementos em um arquivo leva a Varredura de Correio Eletrônico a identificar o arquivo como potencialmente infectado com um vírus novo ou que não foi identificado anteriormente.

Como a Varredura de Correio Eletrônico procura simultaneamente as características de arquivo que excluam a possibilidade de infecção por vírus, raramente será dada uma informação falsa. Entretanto, a menos que você saiba que esse arquivo **não** contém um vírus, deverá tratar as infecções "prováveis" com o mesmo cuidado que as confirmadas.

Para ativar a varredura heurística, siga estas etapas

a. Marque a caixa de verificação **Ativar a varredura heurística**. As demais opções na caixa de diálogo são ativadas.

b. Selecione os tipos de varredura heurística que devem ser utilizadas pela Varredura de Correio Eletrônico. Estas são as opções:

- **Ativar a varredura heurística de macro**. Escolha esta opção para que a Varredura de Correio Eletrônico identifique todos os arquivos do Microsoft Word, Microsoft Excel e outros do Microsoft Office que tenham macros incorporadas, em seguida compare o código da macro com o banco de dados de assinaturas de vírus. Esse componente identificará as correspondências exatas com o nome do vírus; as assinaturas de código semelhantes àquelas de vírus existentes fazem com que a Varredura de Correio Eletrônico lhe informe que encontrou um provável vírus de macro.
- **Ativar a varredura heurística de arquivos de programa.** Escolha esta opção para que a Varredura de Correio Eletrônico localize vírus em arquivos de programa examinando as suas características e comparando-as a uma lista de especificações de vírus conhecidos. Esse componente identificará os arquivos com um número suficiente dessas características como vírus prováveis.
- **Ativar a varredura heurística de arquivos de programa e macros.** Escolha esta opção para que a Varredura de Correio Eletrônico use ambos os tipos de varredura heurística. A Network Associates recomenda que você use essa opção para obter uma proteção completa antivírus.

c. Determinar como deseja tratar os arquivos de macros infectados. Selecione **Remover todas as macros ao limpar documentos infectados** para eliminar todos os códigos infectantes do documento e deixar apenas os dados. Para tentar eliminar apenas os códigos de vírus das macros de documentos, não marque essa caixa de verificação.

ATENÇÃO: Use esse recurso com cuidado: a remoção de todas as macros de um documento pode causar a perda de dados ou danificá-lo, tornando o documento inútil.

d. Clique em **OK** para salvar as suas configurações e retornar à caixa de diálogo Propriedades da Varredura de Correio Eletrônico.

3. Clique na guia Ação para escolher opções da Varredura de Correio Eletrônico adicionais. Para salvar as suas configurações sem fechar a caixa de diálogo Propriedades da Varredura de Correio Eletrônico, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Ação

Quando a Varredura de Correio Eletrônico detecta um vírus, poderá lhe perguntar o que deve fazer com o arquivo infectado ou atuar automaticamente realizando uma ação predeterminada. Use a página de propriedades Ação para especificar quais opções de ação a Varredura de Correio Eletrônico deve lhe propor ao encontrar um vírus ou quais as ações que o programa deve realizar automaticamente.

Siga estas etapas:

1. Clique na guia Ação, na caixa de diálogo Propriedades da Varredura de Correio Eletrônico, para exibir a página de propriedades correta (Figura 7-5).

Figura 7-5. Caixa de diálogo Propriedades da Varredura de Correio Eletrônico – página Ação

2. Escolha uma ação na lista **Quando um vírus for encontrado**. A área imediatamente abaixo da lista será alterada para mostrar as opções adicionais para cada uma delas. Estas são as opções:

   - **Solicitar ação ao usuário.** Use esta opção se você espera estar utilizando o seu computador enquanto a Varredura de Correio Eletrônico examina o disco — o programa exibirá uma mensagem de alerta quando encontrar um vírus e lhe proporá a sua ampla gama de opções disponíveis. Selecione as opções de ação que você deseja ver na mensagem de alerta:

     – **Limpar arquivo.** Esta opção informa à Varredura de Correio Eletrônico para tentar remover o código de vírus do arquivo infectado.

     – **Excluir arquivo.** Esta opção informa à Varredura de Correio Eletrônico para excluir o arquivo infectado imediatamente.

     – **Mover arquivo.** Esta opção informa à Varredura de Correio Eletrônico para mover o arquivo infectado para um diretório de quarentena.

     – **Continuar a varredura.** Esta opção informa à Varredura de Correio Eletrônico para continuar o exame, mas não atuar de qualquer outra maneira. Se as opções de relatório estiverem ativadas, a Varredura de Correio Eletrônico incluirá a ocorrência no arquivo de registro.

     – **Parar a varredura.** Esta opção também faz com que a Varredura de Correio Eletrônico pare a operação de varredura imediatamente. Para continuar, você deve clicar em **Examinar agora** para reiniciar a operação.

   - **Mover anexos infectados automaticamente**. Use esta opção para que a Varredura de Correio Eletrônico mova os arquivos infectados para um diretório de quarentena chamado INFECTADO. A Varredura de Correio Eletrônico criará a pasta INFECTADO no servidor de correio do Exchange ou Outlook.

     Não é possível especificar uma pasta diferente nem alterar o nome da pasta, mas a pasta INFECTADO aparecerá abaixo de sua caixa de correio. Você pode abrir a pasta e ver as mensagens que quiser, mas observe que isso pode expor o seu computador a infecção por vírus.

- **Limpar anexos infectados automaticamente.** Use esta opção para informar à Varredura de Correio Eletrônico que remova o código do vírus do anexo infectado assim que o encontrar. Se o componente não puder removê-lo, você receberá um aviso através de uma notificação na área de mensagem, e caso os recursos de relatório estiverem ativados, a ocorrência será incluída no arquivo de registro. Veja o “Escolhendo opções de Relatório” na página 254 para obter mais detalhes.
- **Excluir anexos infectados automaticamente.** Use esta opção para que a Varredura de Correio Eletrônico exclua imediatamente os anexos infectados encontrados. Certifique-se de ter ativado o recurso de relatório para que você tenha um registro de quais anexos a Varredura de Correio Eletrônico excluiu. Será necessário restaurar os anexos excluídos a partir de cópias de backup.

  ATENÇÃO: A Varredura de Correio Eletrônico *não* tentará abrir mensagens criptografadas para examiná-las. Se um anexo infectado incluir uma assinatura digital, a Varredura de Correio Eletrônico a *removerá* para limpar ou excluir o arquivo infectado.

- **Continuar a varredura.** Use esta ação se você pretende afastar-se do seu computador enquanto a Varredura de Correio Eletrônico o examina em busca de vírus. Se as opções de relatório da Varredura também estiverem ativadas, o programa (veja “Escolhendo opções de Relatório” na página 254 para obter mais detalhes), registrará os nomes dos vírus e os nomes de arquivos infectados para que você possa excluí-los na próxima oportunidade.

3. Clique na guia Alerta para escolher opções da Varredura de Correio Eletrônico adicionais. Para salvar as suas configurações sem fechar a caixa de diálogo Propriedades da Varredura de Correio Eletrônico, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

   NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Alerta

Após ser configurado com as opções de ação desejadas, a Varredura de Correio Eletrônico irá procurar vírus no sistema e remover automaticamente os encontrados, sem quase nenhuma outra intervenção. Se, contudo, você quiser configurar a Varredura de Correio Eletrônico para avisar-lhe imediatamente após encontrar um vírus, a fim de que você possa realizar a ação necessária, há várias maneiras de configurá-la para enviar uma mensagem de alerta para você. Use a página de propriedades Alerta para escolher quais métodos de alerta deseja utilizar.

Siga estas etapas:

1. Clique na guia Alerta na caixa de diálogo Propriedades da Varredura de Correio Eletrônico para exibir a página de propriedades correta (Figura 7-6).
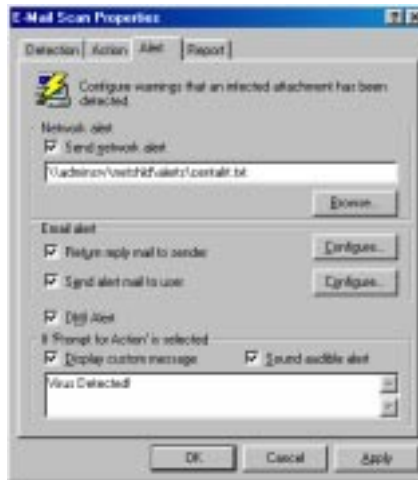
Figura 7-6. Caixa de diálogo Propriedades da Varredura de Correio Eletrônico – página Alerta

2. Para informar à Varredura de Correio Eletrônico que envie uma mensagem de alerta a um servidor que esteja executando o NetShield, uma solução antivírus com base em servidor da Network Associates, marque a caixa de verificação **Enviar alerta de rede**, em seguida, digite o caminho para a pasta de alertas do NetShield na sua rede, ou clique em **Procurar** para localizar a pasta correta.

NOTA: A pasta escolhida deve conter o CENTALRT.TXT, o arquivo Alerta Centralizado do NetShield. Esse programa coleta as mensagens de alerta da Varredura de Correio Eletrônico e de outros softwares da Network Associates, em seguida, passa-as para os administradores de rede a fim de que realizem as ações necessárias. Para saber mais sobre o Alerta Centralizado, veja o *Guia do Usuário* do NetShield

3. Para enviar uma mensagem de alerta para a pessoa que lhe enviou um anexo de correio eletrônico infectado, marque a caixa de verificação **Enviar resposta de correio ao remetente**. Em seguida, você pode compor uma resposta padrão para ser enviada. Siga estas etapas:

   a. Clique em **Configurar** para abrir um formulário de mensagem de correio padrão.

   b. Preencha a linha do assunto, em seguida, adicione os comentários que quiser no corpo da mensagem, abaixo de uma nota sobre a infecção que a Varredura de Correio Eletrônico fornecerá. Podem ser adicionados até 1024 caracteres de texto.

   c. Para enviar uma cópia desta mensagem de correio eletrônico a outra pessoa, digite um endereço de correio eletrônico na caixa de texto mostrada ou clique em **Cc:** para escolher um destinatário na lista de endereços de seu sistema de correio eletrônico.

   d. Clique em **OK** para salvar a mensagem.

   Ao detectar um vírus, a Varredura de Correio Eletrônico enviará uma cópia desta mensagem para cada pessoa que lhe envia correio eletrônico com anexo infectado. O programa preenche o endereço do destinatário com as informações encontradas no cabeçalho da mensagem original, e identifica o vírus e o arquivo infectado na área imediatamente abaixo da linha do assunto. Se o recurso de relatório estiver ativado, a Varredura de Correio Eletrônico também registrará cada ocorrência quando enviar uma mensagem de alerta.

4. Para enviar uma mensagem de correio eletrônico a fim de avisar as pessoas sobre um anexo infectado, marque a caixa de verificação **Enviar mensagem de alerta para o usuário**. Em seguida, componha uma resposta padrão para enviá-la a um ou mais destinatários — um administrador de rede, por exemplo — sempre que a Varredura de Correio Eletrônico detectar um anexo de correio eletrônico infectado. Siga estas etapas:

a. Clique em **Configurar** para abrir um formulário de mensagem de correio padrão.

b. Digite um endereço de correio eletrônico na caixa de texto fornecida ou clique em **Para:** para escolher um destinatário na lista de endereços de seu sistema de correio eletrônico. Repita esse procedimento na caixa de texto rotulada com **Cc:** para enviar uma cópia da mensagem para outra pessoa.

> **NOTA:** Para localizar um endereço de correio eletrônico dessa maneira, você deve ter acesso a um diretório de usuário compatível com MAPI. Se ainda não tiver sido estabelecida a sua conexão com o sistema de correio eletrônico, a Varredura de Correio Eletrônico lhe pedirá que escolha um perfil de usuário que o programa possa usar para conectar-se ao seu sistema. Digite as informações solicitadas, em seguida, clique em **OK** para continuar.

c. Preencha a linha do assunto, em seguida, acrescente os comentários desejados no corpo da mensagem, abaixo do aviso de infecção. Podem ser adicionados até 1024 caracteres de texto.

d. Clique em **OK** para salvar a mensagem.

Ao detectar um vírus, a Varredura de Correio Eletrônico envia uma cópia desta mensagem para cada um dos endereços digitados na Etapa b. O programa adiciona informações para identificar o vírus e o arquivo infectado, na área imediatamente abaixo da linha do assunto. Se o recurso de relatório estiver ativado, a Varredura de Correio Eletrônico também registrará cada ocorrência quando enviar uma mensagem de alerta.

5. Para que a Varredura de Correio Eletrônico envie mensagens de alerta sobre vírus através da interface de componente DMI para aplicativos de gerenciamento de rede ou de computadores de mesa que estejam sendo executados na sua rede, marque a caixa de verificação **Alerta DMI**.

> **NOTA:** A Desktop Management Interface é um padrão para comunicação de solicitações de gerenciamento e informações sobre alertas entre componentes de hardware e software armazenados em ou conectados a computadores de mesa, e os aplicativos utilizados para gerenciá-los. Para saber mais sobre a utilização desse método de alerta, consulte o administrador de rede.

6. Se você escolher **Solicitar ação ao usuário** como a sua opção de ação na página Ação (veja página 249 para obter mais detalhes), também poderá informar à Varredura de Correio Eletrônico que emita um sinal sonoro e exiba uma mensagem personalizada ao encontrar um vírus. Para fazer isso, marque a caixa de verificação **Exibir mensagem personalizada** em seguida, digite a mensagem que aparecerá na caixa de texto mostrada — pode ser digitada uma mensagem com 225 caracteres, no máximo. Depois, marque a caixa de verificação **Soar alerta audível**.

7. Clique na guia Relatório para escolher opções da Varredura de Correio Eletrônico adicionais. Para salvar as suas configurações sem fechar a caixa de diálogo Propriedades da Varredura de Correio Eletrônico, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Escolhendo opções de Relatório

A Varredura de Correio Eletrônico contém uma lista com as configurações atuais e resume todas as ações efetuadas, durante as operações de varredura, em um arquivo de registro chamado MAILSCAN.TXT. A Varredura de Correio Eletrônico poderá gravar o registro nesse arquivo ou usar um arquivo de texto criado com qualquer editor de texto. Esse arquivo de registro pode ser aberto e impresso para revisão posterior na Varredura de Correio Eletrônico ou em qualquer editor de texto.

Use a página de propriedades de Relatório para determinar quais informações a Varredura de Correio Eletrônico incluirá no arquivo de registro.

Para configurar a Varredura de Correio Eletrônico a fim de registre suas ações em um arquivo de registro, siga estas etapas

1. Clique na guia Relatório na caixa de diálogo Propriedades da Varredura de Correio Eletrônico para exibir a página de propriedades correta (Figura 7-7).

Figura 7-7. Caixa de diálogo Propriedades da Varredura de Correio Eletrônico – página Relatório

2. Marque a caixa de verificação **Registrar no arquivo**.

   Como padrão, a Varredura de Correio Eletrônico grava as informações sobre registro no arquivo MAILSCAN.TXT no diretório de programa do VirusScan. Você pode digitar um nome diferente na caixa de texto mostrada, ou clique em **Procurar** para localizar um arquivo adequado no disco rígido ou na rede.

3. Para minimizar o tamanho do arquivo de registro, marque a caixa de verificação **Limitar tamanho do arquivo de registro em** e digite um valor para o tamanho do arquivo, em quilobytes, na caixa de texto mostrada.

   Digite um valor entre 10Kb e 999Kb. Como padrão, a Varredura de Correio Eletrônico limita o tamanho do arquivo em 100Kb. Se os dados no arquivo de registro excederem o tamanho de arquivo configurado, a Varredura de Correio Eletrônico apagará o registro já existente e iniciará outro a partir do ponto de interrupção.

4. Marque as caixas de verificação correspondentes às informações que a Varredura de Correio Eletrônico deverá incluir no arquivo de registro. Você pode optar por registrar quaisquer destas informações:

   - **Detecção de vírus .** Marque esta caixa de verificação para que a Varredura de Correio Eletrônico anote o número de arquivos infectados, encontrados durante esta sessão de varredura.

   - **Limpeza de vírus.** Marque esta caixa de verificação para que a Varredura de Correio Eletrônico anote o número de arquivos infectados dos quais removeu os vírus.

   - **Eliminação do arquivo infectado.** Marque esta caixa de verificação para que a Varredura de Correio Eletrônico anote o número de arquivos infectados excluídos do servidor de correio eletrônico.

   - **Movimentação do arquivo infectado.** Marque esta caixa de verificação para que a Varredura de Correio Eletrônico anote o número de arquivos infectados que foram movidos para o diretório de quarentena no servidor de correio eletrônico.

   - **Configurações da sessão.** Marque esta caixa de verificação para que a Varredura de Correio Eletrônico faça uma lista das opções escolhidas na caixa de diálogo Propriedades da Varredura de Correio Eletrônico para cada sessão de varredura.

   - **Resumo da sessão.** Marque esta caixa de verificação para que a Varredura de Correio Eletrônico faça um resumo das suas ações durante cada sessão de varredura. As informações do resumo incluem o número de arquivos examinados, o número e o tipo de vírus detectados, o número de arquivos movidos ou excluídos, e outras informações.

- **Data e hora.** Marque esta caixa de verificação para que a Varredura de Correio Eletrônico anexe a data e a hora a cada entrada do registro incluída.

- **Nome do usuário.** Marque esta caixa de verificação para que Varredura de Correio Eletrônico anexe o nome do usuário conectado ao servidor de correio eletrônico no momento que incluir cada entrada de registro.

5. Clique em uma guia diferente para alterar as configurações da Varredura de Correio Eletrônico. Para salvar as suas configurações sem fechar a caixa de diálogo Propriedades da Varredura de Correio Eletrônico, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

Varredura do cc:Mail

O VirusScan inclui suporte nativo para software de cliente de correio eletrônico de última geração com base no padrão MAPI da Microsoft, inclusive para os clientes Exchange e Outlook da Microsoft, e para a versão 8.0 e posteriores do produto cc:Mail da Lotus Development. Se você utilizar as versões anteriores do cc:Mail — v6.0 ou v7.0 — precisará instalar o componente Varredura do cc:Mail do VirusScan para procurar vírus em sua Caixa de Entrada.

IMPORTANTE: Para instalar o componente Varredura do cc:Mail, você deve escolher a opção de instalação Personalizada durante a configuração — o VirusScan não instala esse componente como padrão. Veja o página 43 para obter mais detalhes.

Quando é instalada a Varredura do cc:Mail Scan conecta-se ao VShield e ao seu sistema cc:Mail, em seguida opera discretamente em segundo plano, fazendo consulta seqüencial da sua Caixa de Entrada do cc:Mail para verificar as novas mensagens de correio. Quando chega novo correio, a Varredura do cc:Mail chama o VShield para examiná-lo em busca de qualquer anexo de arquivo infectado antes que o software de cliente faça download do correio para o seu computador.

A única real interação entre você e a Varredura do cc:Mail Scan se dá ao escolher qual o sistema de correio eletrônico corporativo o VShield deverá examinar em busca de vírus. Para saber como especificar cc:Mail como um sistema de correio eletrônico corporativo, veja Capítulo 4, página 109.

Caso ainda não tenha se conectado ao servidor do cc:Mail, a Varredura do cc:Mail Scan deverá também lhe solicitar que digite o seu nome de usuário e a senha em uma tela de conexão para que o VShield possa ter acesso ao seu servidor do cc:Mail e examinar a sua Caixa de Entrada. Digite o seu nome de usuário do cc:Mail e a senha, como se estivesse conectando-se diretamente no cc:Mail, em seguida, clique em **OK** para continuar. Depois, inicie o aplicativo de cliente cc:Mail, em seguida, defina o intervalo para o cliente fazer consulta seqüencial no servidor do cc:Mail para um período maior que 5 minutos. Este procedimento dá ao VShield a chance de examinar o seu correio antes que o software de cliente o recupere.

O componente cc:Mail desconecta-se do servidor de correio eletrônico quando você encerra o software de cliente.

Usando o ScreenScan

O componente ScreenScan do VirusScan faz uma varredura em segundo plano para procurar vírus, enquanto o protetor de tela do computador estiver em ação. Com esse componente, você pode transformar o tempo ocioso do computador em uso produtivo permitindo que a sua máquina faça uma autoverificação para procurar infecções por vírus. O ScreenScan não atua contra os vírus detectados, mas registra os resultados de suas operações de varredura em um arquivo de registro que você poderá rever quando puder.

Para usar o ScreenScan, você deve escolher a instalação Personalizada durante o programa de instalação — o VirusScan não instala esse componente como padrão. Veja o página 42 para obter mais detalhes. Uma vez instalado, o ScreenScan exibe uma página de propriedades na caixa de diálogo Exibir propriedades do Windows. Nessa caixa de diálogo, você pode escolher as opções de detecção e relatório que o ScreenScan usará.

Para configura o ScreenScan, siga estas etapas:

1. Clique em **Iniciar** na barra de tarefas do Windows, aponte para **Configurações**, em seguida, escolha **Painel de Controle**.

2. Localize e clique duas vezes no painel de controle Vídeo na janela mostrada para abrir a caixa de diálogo Propriedades de Vídeo. Depois, clique na guia McAfee ScreenScan para exibir a página de propriedades correta (veja Figura 7-8 na página 259).
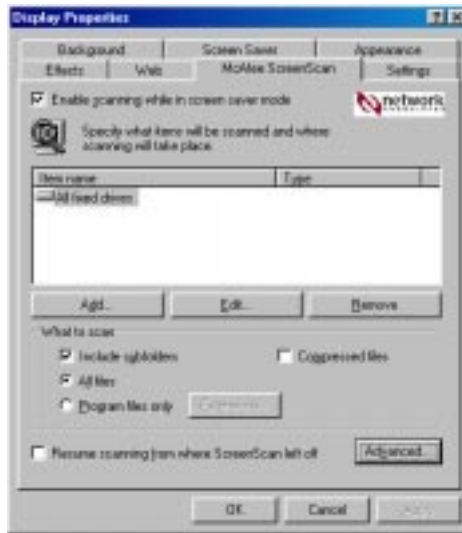
Figura 7-8. Caixa de diálogo Propriedades de Vídeo - página McAfee ScreenScan

3. Marque a caixa de verificação **Ativar a varredura no modo de proteção de tela** para ativar as opções no restante da página de propriedades.

4. Escolha em quais partes do sistema o ScreenScan deverá procurar vírus. Você pode

   - **Adicionar destinos de varredura.** Clique em **Adicionar** para abrir a caixa de diálogo Adicionar item de varredura (Figura 7-9).

Figura 7-9. Caixa de diálogo Adicionar item de varredura

Em seguida, escolha o destino na lista fornecida. Estas são as opções:

– **Todas as unidades locais.** Esta opção informa ao ScreenScan que examine todas as unidades, discos rígidos e unidades de disquete, fisicamente anexados ao computador ou inseridos em uma unidade de disco. Esta é a mais completa e segura opção no ScreenScan.

– **Todos os discos rígidos.** Esta opção informa ao ScreenScan que examine apenas os discos rígidos fisicamente anexados ao computador.

– **Unidade ou pasta.** Esta opção instrui o ScreenScan a examinar uma determinada pasta ou disco no seu computador. Na caixa de texto mostrada, digite a letra da unidade ou o caminho para a pasta a ser examinada, ou clique em **Pesquisar** para localizar o destino da varredura no computador. Clique em **OK** fechar a caixa de diálogo.

> **IMPORTANTE:** Para examinar todas as subpastas no destino de varredura, verifique se a caixa de verificação **Incluir subpastas** está marcada na área **O que examinar** na página de propriedades do ScreenScan.

- **Alterar destinos de varredura.** Selecione um dos destinos de varredura na lista, em seguida clique em **Editar** para abrir a caixa de diálogo Editar item para varredura (Figura 7-10).

Figura 7-10. Caixa de diálogo Editar item para varredura

A caixa de diálogo aparece com o destino de varredura especificado. Escolha ou digite um novo destino de varredura, em seguida, clique em **OK** para fechar a caixa de diálogo.

- **Remover destinos de varredura.** Selecione um dos destinos de varredura na lista, em seguida, clique em **Remover** para excluí-lo.

5. Especificar os arquivos que o ScreenScan examinará. Você pode

   - Examinar arquivos compactados. Marque a caixa de verificação **Arquivos compactados** para que o ScreenScan procure vírus em arquivos compactados nos formatos de arquivamento .CAB, LZH ou .ZIP.

- **Escolher tipos de arquivos para varredura.** Os vírus normalmente não podem infectar arquivos de dados ou que não contenham código executável. Contudo, você pode reduzir seguramente a abrangência das operações de varredura para que o ScreenScan observe apenas os anexos mais suscetíveis a infecções por vírus. Para fazê-lo, selecione o botão **Somente arquivos de programa**. Para ver ou designar as extensões de nomes de arquivos que o ScreenScan examinará, clique em **Extensões** para abrir a caixa de diálogo Extensões de arquivo de programa (veja Figura 7-11).
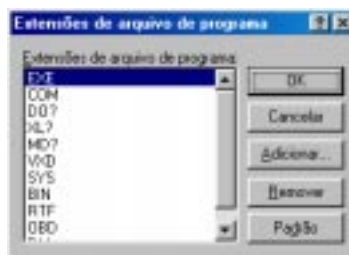
Figura 7-11. Caixa de diálogo Extensões de arquivo de programa

Como padrão, o ScreenScan procura vírus em arquivos com as extensões .EXE, .COM, .DO?, .XL?, .MD?, .RTF, .BIN, .SYS, .VXD, .OBD e .DLL. Os arquivos com as extensões .DO?, .XL?, .RTF e .OBD pertencem ao Microsoft Office, sendo que todos podem ser infectados por vírus de macro. O ? é um curinga que possibilita ao VirusScan examinar arquivos de modelos e de documentos.

– Para adicionar extensões na lista, clique em **Adicionar**, em seguida, digite as extensões que o ScreenScan deverá examinar, na caixa de diálogo mostrada.

– Para remover uma extensão da lista, selecione-a, em seguida, clique em **Remover**.

– Clique em **Padrão** para restaurar a lista à sua forma original.

Ao terminar, clique em **OK** para fechar a caixa de diálogo.

Para que o ScreenScan examine todo os arquivos no seu sistema, com qualquer extensão, selecione o botão **Todos os arquivos**. Embora este procedimento ofereça mais proteção, tornará as operações de varredura consideravelmente mais lentas.

6. Determine qual a prioridade das operações de varredura do ScreenScan em relação a outras prioridades de trabalho do seu computador. Clique em **Avançado** para abrir a caixa de diálogo Configurações de varredura avançadas (Figura 7-12).

Figura 7-12. Caixa de diálogo Configurações de varredura avançadas

Arraste o botão deslizante para a esquerda para que o ScreenScan tenha uma prioridade baixa em relação a outros programas em execução no seu computador — incluindo o protetor de tela. Isto faz com que o ScreenScan gaste mais tempo para examinar o sistema, mas permite que outros programas sejam executados ao mesmo tempo. Arraste o botão deslizante para a direita para que o ScreenScan tenha uma prioridade relativamente alta para as suas tarefas de varredura. Essas operações serão concluídas mais rapidamente, mas outros programas que estejam sendo executados ao mesmo tempo podem não funcionar harmoniosamente.

7. Ativar o recurso de relatório do ScreenScan.

Marque a caixa de verificação **Ativar o registro de atividades do ScreenScan para um arquivo**. Como padrão, o ScreenScan registra suas ações em um arquivo de texto chamado SCREENSCAN ACTIVITY LOG.TXT. Para escolher um arquivo de texto diferente para usar como arquivo de relatório do ScreenScan, digite o caminho e o nome do arquivo na caixa de texto mostrada ou clique em **Procurar** para localizar um arquivo adequado no seu disco rígido.

NOTA: O ScreenScan não cria novos arquivos de relatório. Para que o programa use um arquivo de registro diferente, escolha um arquivo de texto já existente que ScreenScan possa abrir e gravar seus registros.

Clique em **OK** para salvar as alterações e fechar a caixa de diálogo. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

8. Para que o ScreenScan comece a varredura a partir do ponto de interrupção, marque a caixa de verificação **Continuar a varredura onde o ScreenScan**. Se esta caixa de verificação não for marcada, o ScreenScan iniciará a operação de varredura no primeiro item da lista de destinos de varredura escolhidos, já tendo ou não concluído um exame desse item.

9. Para salvar as suas configurações sem fechar a caixa de diálogo Propriedades de Vídeo, clique em **Aplicar**. Para salvar as alterações e fechar a caixa de diálogo, clique em **OK**. Para fechar a caixa de diálogo sem salvar as suas configurações, clique em **Cancelar**.

NOTA: O clique em **Cancelar** não irá desfazer as alterações já salvadas com **Aplicar**.

O ScreenScan será ativada na próxima vez que o se protetor atual entrar em execução. Se você trocar de protetor de tela, deverá reconfigurar também as opções do ScreenScan.

Usando o SecureCast para atualizar o software

Introdução ao SecureCast

O serviço Secure Cast da Network Associates entrega, para a sua conveniência, as mais recentes atualizações de arquivos de dados e do produto na sua área de trabalho. Com este serviço, você pode escolher se deseja receber as atualizações para o seu software licenciado da Network Associates via Internet, com regularidade e automaticamente. Para usar essa opção, é necessário instalar o software de cliente SecureCast e tornar-se assinante do canal Home SecureCast (para clientes do varejo) ou o canal Enterprise SecureCast (para clientes corporativos).

Se você é um cliente varejista e prefere decidir quando deseja atualizar o seu sistema, uma opção permite descarregar os novos arquivos quando o software lhe lembrar que chegou o momento de atualizá-lo. Os clientes corporativos (mas não um administrador) devem entrar em contato com os seus administradores para saber onde atualizar os arquivos, ou usar o recurso Atualização automática se o produto o incluir.

Escolha uma das opções de atualização, contidas em uma lista, neste apêndice para manter o sistema protegido eficientemente na rede ou no computador de mesa. Com o SecureCast, você obterá os mais recentes arquivos de dados e de programa assim que estiverem disponíveis. Novos vírus e outros agentes nocivos aparecem com uma freqüência de mais de 200 por mês — não se arrisque a deixar que seus dados se desintegrem ou que a rede torne-se inacessível simplesmente por que se esqueceu de atualizar os arquivos de dados ou a versão do software.

NOTA: O termo "atualizar" significa integrar o produto com novas versões de arquivos (.DAT) de dados; o termo "atualizar a versão" refere-se às revisões da versão do produto, dos arquivos executáveis e de dados. A Network Associates oferece atualizações gratuitas dos arquivos .DAT de dados durante a vida do produto. Porém, isso não garante que esses arquivos serão compatíveis com as versões anteriores do produto. Ao atualizar o software para a versão mais recente e atualizar para os arquivos .DAT de dados mais recentes, regularmente através do SecureCast, é assegurada a completa proteção durante o período de duração da assinatura do software ou do plano de manutenção.

Por que é necessário atualizar os arquivos de dados?

Para lhe oferecer a melhor proteção possível, a Network Associates atualiza continuamente os arquivos de dados que detectam novos vírus e outros agentes destrutivos. Embora o software contenha tecnologia que permite detectar previamente linhagens de vírus desconhecidas ou código destrutivo, os novos tipos de vírus e outros agentes aparecem com freqüência. Algumas vezes o software não consegue detectar esses invasores porque os arquivos de dados que o acompanham tornaram-se desatualizados. O software lhe avisa periodicamente para atualizar esses arquivos. Para obter máxima proteção, a Network Associates recomenda enfaticamente que as atualizações sejam regulares.

Quais são os arquivos de dados fornecidos pelo SecureCast?

Com o SecureCast, você receberá automaticamente por download esses arquivos de dados comuns:

- NAMES.DAT — inclui nomes de vírus e outros detalhes exibidos na Lista de vírus.
- SCAN.DAT — inclui os dados da cadeia de caracteres de detecção para todos os vírus detectados.
- CLEAN.DAT — inclui os dados da cadeia de caracteres de remoção para todos os vírus removidos.

Além dos arquivos .DAT comuns, acima, é possível também receber alguns destes arquivos adicionais, dependendo de qual produto antivírus ou de segurança estiver sendo executado:

- WEBSCANX.DAT ou INTERNET.DAT — inclui dados da cadeia de caracteres de detecção para miniaplicativos Java e controles ActiveX hostis. O WebShieldX e o VirusScan usam esses arquivos.
- MCALYZE.DAT — inclui os dados da cadeia de caracteres de detecção para detectar vírus polimorfos complexos. Os produtos de 32 bits com as versões 3.0.0 a 3.1.4 de mecanismos da Network Associates usam esse arquivo.
- POLYSCAN.DAT — inclui os dados da cadeia de caracteres de detecção para detectar vírus polimorfos complexos. Os produtos de 32 bits com as versões 3.1.5 e posteriores de mecanismos da Network Associates usam esse arquivo.

Requisitos de sistema

- Windows 95 ou posterior, ou Windows NT
- Pelo menos 100 MB de espaço livre em disco: Home SecureCast (cliente e canal) 7MB, mais 3 a 6MB por download. Enterprise SecureCast (cliente e canal) 15MB, mais 6 a 6.5MB por download.
- Uma conexão de Internet ativa — direta ou de discagem — com uma hora por semana, no mínimo.

Recursos do SecureCast

- O SecureCast usa software de cliente desenvolvido com as tecnologias BackWeb.
- O SecureCast elimina a necessidade de fazer download de arquivos de atualização nos serviços eletrônicos da Network Associates.
- O SecureCast funciona de modo invisível, em segundo plano, permitindo que outros aplicativos tenham prioridade e usando a sua conexão com a Internet quando estiver ociosa. O cliente de computador de mesa também pode ser configurado para que os downloads do SecureCast tenham uma prioridade mais alta.
- O SecureCast funciona com a maioria das barreiras de proteção corporativas.
- O SecureCast aceita as conexões de TCP/IP de 32 bits para os assinantes dos canais Enterprise SecureCast e Home SecureCast, além de fornecer conexões diferentes de Internet para usuários individuais que usam discagem de modem assíncrona.
- O SecureCast fornece arquivos .ZIP, .EXE e .DAT para a sua área de trabalho como BackWeb InfoPaks.

Serviços gratuitos

- Entrega automática de arquivos .DAT. Normalmente, os arquivos .DAT estão disponíveis na primeira quinzena do mês.
- Alertas sobre vírus perigosos recentemente identificados.
- Anúncios de novas versões do software e produtos associados.

Canal Home SecureCast

Os clientes individuais podem instalar o software de cliente SecureCast com o CD-ROM da Network Associates.

Compreendendo o SecureCast

Se você for um cliente varejista, poderá usar o serviço SecureCast de entrega gratuita, de uma das seguintes maneiras:

- Para receber downloads automáticos das atualizações mais recentes do software licenciado da Network Associates através da Internet, instale o cliente SecureCast, em seguida, faça uma assinatura do canal Home SecureCast; ou
- Se você prefere decidir quando deve atualizar o software, use o utilitário de atualização incluído quando o software lhe lembrar que chegou o momento de atualizá-lo.

Fazendo download automático

Configurando o Home SecureCast

Para assinar o canal Home SecureCast, siga estas etapas:

1. Instale o software de cliente BackWeb da Network Associates CD-ROM.

   Você receberá um Welcome InfoPak que lhe informa que a sua conexão com o canal Home SecureCast está funcionando. Um InfoPak pode conter sons, animações, páginas da Web e muito mais. Ao receber um novo InfoPak do Home SecureCast, este aparecerá automaticamente como um objeto animado na sua área de trabalho até que seja aberto. Para abrir um InfoPak, basta clicar nele duas vezes.

2. Conclua o processo de registro do canal, na caixa de diálogo Informações sobre registro do usuário (que aparecerá no primeiro ou segundo InfoPak recebido), em seguida, clique em **Avançar**.

   A caixa de diálogo Status da atividade online controla o status da transmissão dos seus dados.

3. Quando o registro do usuário estiver completo, anote o seu número de registro, em seguida, clique em **Concluir**.

Usando o Home SecureCast

Agora, você já está pronto para receber os Alertas de vírus e as atualizações de arquivos e de versão periódicos. Após alguns dias, serão enviados InfoPaks adicionais. Clique neles duas vezes para extrair e instalar as atualizações do produto ou de suas versões contidas nos InfoPaks.

Cancelando a assinatura do Home SecureCast

Para cancelar este serviço a qualquer momento, siga estas etapas:

1. Clique duas vezes no ícone do cliente SecureCast na área de status da barra de tarefas do Windows.
2. Clique com o botão direito no botão do canal **Doméstico**.

   Aparece um menu de atalho.
3. Clique em **Cancelar assinatura**, em seguida, clique em **OK** para confirmar.

Iniciando um download

Atualizando o software registrado

O software da Network Associates inclui um recurso que lembra a você periodicamente para atualizar o software. Se já tiver decorrido muitos meses desde que o software foi instalado pela primeira vez, a Network Associates recomenda enfaticamente que sejam utilizadas as opções de atualização descritas nas seções seguintes para assegurar que estão sendo usados os arquivos de dados e as versões disponíveis mais recentes.

Atualizando a instalação

Após instalar o software antivírus ou de segurança, a caixa de diálogo Bem-vindo (Figura A-1 na página 270) avisa-lhe para atualizá-lo. Essa caixa de diálogo também aparece quando é iniciado um sistema de computador pré-carregado com o software da Network Associates, pela quinta vez. O McAfee VirusScan, por exemplo, exibe este aviso:

Figura A-1. Caixa de diálogo Bem-vindo

1. Clique em **Atualizar** para receber gratuitamente a versão mais recente do software.

   Aparece a caixa de diálogo Acesso à Internet (Figura A-2).

Figura A-2. Caixa de diálogo Acesso à Internet

2. Se você tiver acesso à Internet, selecione **Sim**, em seguida, clique em **Avançar**. Caso contrário, selecione **Não**, em seguida, clique em **Avançar**.

   - Se tiver selecionado **Sim**, aparece a caixa de diálogo Registro do usuário (Figura A-3).

Figura A-3. Caixa de diálogo Registro do usuário

Preencha as informações solicitadas. Para mover-se entre as caixas de texto, pressione TAB no teclado. Ao terminar, clique em **Avançar>**.

   - Caso tenha selecionado **Não**, aparecerá a caixa do servidor de download (Figura A-4 na página 272). Nessa caixa, você deverá digitar ou confirmar o código do seu país e o código de área, em seguida, escolha o servidor de discagem mais próximo de onde estiver.

Figura A-4. Caixa de diálogo Servidor

❑ **NOTA:** O download dos arquivos .DAT nos servidores de discagem da Network Associates podem aumentar as suas tarifas de chamadas telefônicas de longa distância.

Ao terminar, clique em **Avançar>** para continuar.

O sistema conecta-se a um servidor da Network Associates.

- Se o servidor não contiver novas atualizações de arquivos .DAT ou de versões do software, a caixa de diálogo Status da atividade online (Figura A-5) lhe informa que seus arquivos estão atualizados.
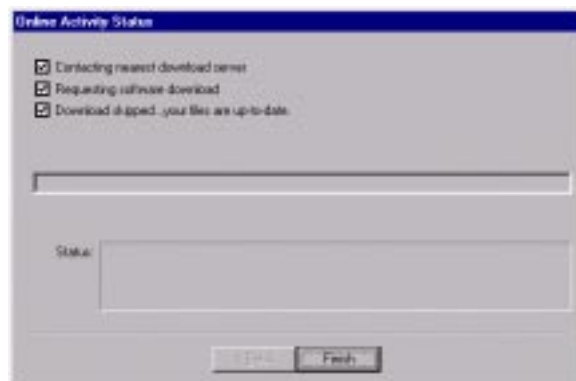
Figura A-5. Caixa de diálogo Status da atividade online (Nenhum Download)

Clique em **Concluir** para desconectar-se do servidor.

- Se o servidor contiver novos arquivos .DAT, a caixa de diálogo Status da atividade online (Figura A-6) lhe informa que o arquivo .EXE contendo os arquivos .DAT está sendo descarregado no seu sistema automaticamente.
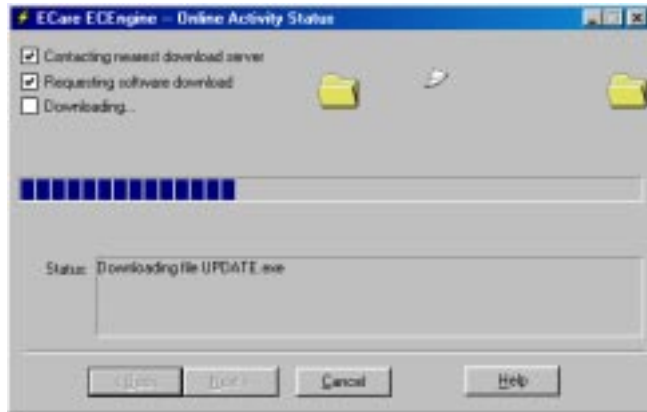
Figura A-6. Caixa de diálogo Status da atividade online

a. Quando o download estiver completo, clique em **Avançar**. Aparece a caixa de diálogo Atividade online concluída (Figura A-7).

Figura A-7. Caixa de diálogo Atividade online concluída

b. Clique em **Concluir** para instalar as atualizações dos novos arquivos .DAT.

- Se o servidor contiver uma versão do produto mais recente que a sua, aparecerá a caixa de diálogo Encontrado componente mais novo (Figura A-8). Para fazer download somente dos arquivos .DAT mais recentes, selecione **Somente arquivos .DAT**, em seguida, clique em **Avançar**. Para fazer download de uma nova versão do produto, clique em **Avançar**.

Figura A-8. Caixa de diálogo Encontrado componente mais novo

A caixa de diálogo Status da atividade online (veja a Figura A-6 na página 273) controla o status do download. Quando estiver completo, clique em **Avançar** para continuar.

A caixa de diálogo Atividade online concluída (Figura A-9) confirma que o download está completo.
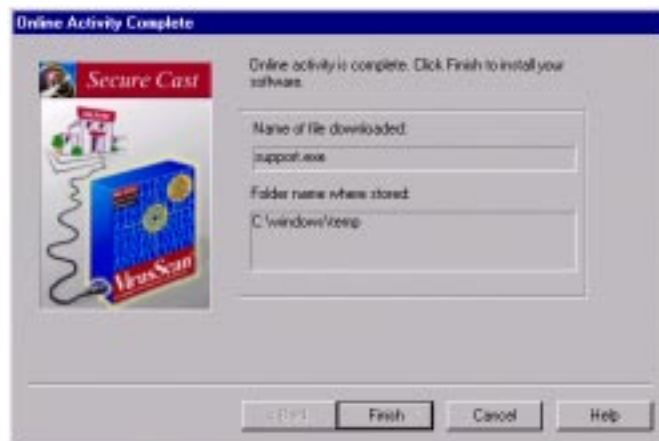
Figura A-9. Caixa de diálogo Atividade online concluída

3. Anote o nome e a localização do arquivo obtido por download, em seguida, clique em **Concluir** para instalar o software.

Atualizando em intervalos periódicos

A intervalos de 30 dias, a caixa de diálogo Atualizar (Figura A-10) avisará que o software deve ser atualizado.

Figura A-10. Caixa de diálogo Atualizar

Se você for um usuário registrado, complete as seguintes etapas para receber gratuitamente as versões mais recentes dos arquivos de dados. Repita estas etapas mensalmente quando o software sugerir que é necessário atualizar o produto.

NOTA: Sendo um usuário registrado, você poderá continuar a receber atualizações dos arquivos .DAT durante a vida do produto. Contudo, a Network Associates não pode garantir a compatibilidade entre futuras atualizações dos arquivos .DAT e as versões mais antigas do produto. Ao adquirir as atualizações de versão do software mais recentes, através do SecureCast, você estará assegurando uma proteção contra vírus completa durante o prazo de duração da assinatura do software ou do plano de manutenção.

---

1. Clique em **Atualizar** para receber gratuitamente a versão mais recente do arquivo de dados.

   Aparece a caixa de diálogo Acesso à Internet (veja a Figura A-2 na página 270).

2. Se você tiver acesso à Internet, selecione **Sim**, em seguida, clique em **Avançar**. Caso contrário, selecione **Não**, em seguida, clique em **Avançar**.

   Aparece a caixa de diálogo Servidor (veja a Figura A-4 na página 272). Se tiver selecionado **Sim**, a caixa do número de discagem não estará disponível; se tiver selecionado **Não**, essa caixa estará disponível.

3. Se você tiver acesso à Internet, verifique o seu Código de país e o Código de área, em seguida, clique em **Avançar**. Caso você não tenha acesso à Internet, verifique o seu Código de País e o Código de Área, selecione um número de discagem de modem, em seguida clique em **Avançar**.

   O sistema conecta-se a um servidor da Network Associates.

   - Se o servidor não contiver novas atualizações de arquivos .DAT ou de versões do software, a caixa de diálogo Status da atividade online (veja a Figura A-5 na página 272) lhe informa que os seus arquivos estão atualizados. Clique em **Concluir** para desconectar-se do servidor.

   - Se o servidor contiver novos arquivos .DAT, a caixa de diálogo Status da atividade online (veja a Figura A-6 na página 273) lhe informa que o arquivo .EXE, contendo os arquivos .DAT, está sendo descarregado no seu sistema automaticamente.

     Quando o download estiver completo, clique em **Avançar**. Aparece a caixa de diálogo Atividade online concluída (veja a Figura A-7 na página 273).

4. Clique em **Concluir** para instalar as atualizações dos novos arquivos .DAT.

Se o servidor tiver uma versão do *produto* mais recente do que a sua, aparece a caixa de diálogo Encontrado componente mais novo (veja a Figura A-8 na página 274).

1. Para fazer download dos arquivos .DAT mais recentes, em vez do produto inteiro, selecione **Somente arquivos DAT**, em seguida, clique em **Avançar**. Para fazer download de uma nova versão do produto, clique em **Avançar**.

2. A caixa de diálogo Status da atividade online (veja a Figura A-6 na página 273) controla o status do download. Quando estiver completo, clique em **Avançar** para continuar.

   A caixa de diálogo Atividade online concluída (Figura A-11) confirma que o download está completo.

Figura A-11. Caixa de diálogo Atividade online concluída

3. Anote o nome e a localização do arquivo obtido por download, em seguida, clique em **Concluir** para instalar o software.

Registrando o software de avaliação

Se você estiver usando uma versão de avaliação do software da Network Associates válida por 30 dias, aparece a caixa de diálogo Adquirir (Figura A-12). Essa caixa de diálogo também é mostrada quando **Adquirir** é escolhida no menu **Arquivo** do produto de software da Network Associates.

Figura A-12. Caixa de diálogo Adquirir

Se você continuar a usar cópias de avaliação do software da Network Associates depois que a licença expirar, após 30 dias, aparecerão lembretes cada vez mais freqüentes de que o software precisa ser registrado. A Network Associates recomenda enfaticamente que você siga estas etapas para assegurar que está utilizando os mais novos arquivos de dados e as versões do produto disponíveis:

1. Na caixa diálogo Adquirir (Figura A-12 na página 277), clique em **Adquirir** para começar a registrar a sua cópia de avaliação do software antivírus eletronicamente.

   Aparece a caixa de diálogo Acesso à Internet (veja a Figura A-2 na página 270).

2. Se você tiver acesso à Internet, selecione **Sim**, em seguida, clique em **Avançar**. Caso contrário, selecione **Não**, em seguida, clique em **Avançar**.

   Aparece a caixa de diálogo Servidor (veja a Figura A-4 na página 272). Se tiver selecionado **Sim**, a caixa do número de discagem não estará disponível; se tiver selecionado **Não**, essa caixa estará disponível.

3. Se você tiver acesso à Internet, verifique o seu Código de país e o Código de área, em seguida, clique em **Avançar**. Caso você não tenha acesso à Internet, verifique o seu Código de País e o Código de Área, selecione um número de discagem de modem, em seguida clique em **Avançar**.

   O sistema conecta-se a um servidor da Network Associates.

   - Se o servidor não contiver novas atualizações de arquivos .DAT ou de versões do software, a caixa de diálogo Status da atividade online (veja a Figura A-5 na página 272) lhe informa que os seus arquivos estão atualizados. Clique em **Concluir** para desconectar-se do servidor.

   - Se o servidor contiver novos arquivos .DAT, a caixa de diálogo Status da atividade online (veja a Figura A-6 na página 273) lhe informa que o arquivo .EXE, contendo os arquivos .DAT, está sendo descarregado no seu sistema automaticamente.

     Quando o download estiver completo, clique em **Avançar**. Aparece a caixa de diálogo Atividade online concluída (veja a Figura A-7 na página 273).

4. Clique em **Concluir** para instalar as atualizações dos novos arquivos .DAT.

Se o servidor tiver uma versão do produto mais recente do que a sua, aparece a caixa de diálogo Encontrado componente mais novo (veja a Figura A-8 na página 274). Para fazer download dos arquivos .DAT mais recentes, em vez do produto inteiro, selecione **Somente arquivos DAT**, em seguida, clique em **Avançar**. Para fazer download de uma nova versão do produto siga estas etapas:

1. Clique em **Avançar** para obter a versão mais nova do software.

   Se você não tiver mais direito a atualizações de versão gratuitas do software, aparece uma segunda caixa de diálogo Encontrado componente mais novo (Figura A-13).

Figura A-13. Caixa de diálogo no. 2 Encontrado componente mais novo

---

NOTA: Os tamanhos de arquivos e os preços do suporte são gerados dinamicamente. O que você vê quando faz download da sua aquisição, contudo, pode ser diferente do que aparece na Figura A-13.

---

2. Clique em **Avançar>** para continuar o download.

   A caixa de diálogo Digitar informações sobre cartão de crédito (Figura A-14 na página 280) aparece.

Figura A-14. Caixa de diálogo Digitar informações sobre cartão de crédito

3. Digite o endereço de cobrança do seu cartão de crédito, número da conta e data de validade. Clique em **Avançar>** para continuar.

❑ **NOTA:** Os detalhes sobre o seu cartão de crédito são transmitidos em uma transação segura.

A caixa de diálogo Autorização de compra online (Figura A-15) aparece.

Figura A-15. Caixa de diálogo Autorização de compra online

4. Marque a caixa de verificação para autorizar o débito da transação no seu cartão de crédito e clique em Clique aqui para comprar a fim de iniciar o processo de download.

   NOTA: A Network Associates não debitará o valor no seu cartão de crédito a não ser que o download seja concluído com sucesso.

   A caixa de diálogo Status da atividade online (veja a Figura A-6 na página 273) controla o status do download.

5. Quando o download estiver completo, anote o número da transação resultante para a sua aquisição, em seguida, clique em **Avançar>** para continuar.

   A caixa de diálogo Atividade online concluída (veja a Figura A-9 na página 274) confirma que a transação está completa.

6. Anote o nome e a localização do arquivo obtido por download, em seguida, clique em **Concluir** para instalar o software.

Canal Enterprise SecureCast

Se você administra uma rede corporativa, deve fazer download do software de cliente do BackWeb no site corporativo da Network Associates (http://www.nai.com) e instalá-lo em um servidor de rede. O Enterprise SecureCast destina-se ao uso somente por administradores, e não por usuários finais corporativos.

NOTA: Quando o primeiro InfoPak chegar, clique nele duas vezes para abri-lo, em seguida, conclua o processo de registro do canal através das caixas de diálogo Informações sobre registro de cliente. Quando você receber os arquivos do InfoPak subseqüentes do Enterprise SecureCast, a Network Associates recomenda enfaticamente que sejam distribuídos a computadores de mesa individuais, conforme necessário, para preservar a largura da banda da rede.

Vantagens

- Fácil de usar

  Você não precisará mais procurar e fazer download das atualizações nos serviços de distribuição eletrônicos da Network Associates. As atualizações necessárias serão entregues em formato compactado, prontas para instalação e teste no site.

- Proteção conveniente

  A Network Associates lhe oferece uma proteção conveniente, distribuindo regularmente as atualizações dos arquivos .DAT e de versão do produto diretamente na sua área de trabalho. Logo que as atualizações são colocadas no servidor do SecureCast, começam a ser transferidas para o seu site.

- Alertas de vírus

  Você receberá Alertas de vírus que avisam sobre existência de vírus ameaçadores e sugerem o melhor modo de prevenir contra uma infecção. Além disso, os alertas que distinguem as brincadeiras inconseqüentes das ameaças sérias economizam o seu valioso tempo e evitam preocupações desnecessárias.

- Atualizações de versão para diversas plataformas

  Uma assinatura do Enterprise SecureCast permite que você receba atualizações e atualizações de versão dos seus produtos para diversas plataformas. As atualizações de arquivos e as atualizações de versão dos produtos da Network Associates executados no Windows 95, Windows 98, Windows NT, Windows 3.*x*, DOS, OS/2 e Mac OS podem ser distribuídas para a sua área de trabalho.

- Versões em diversos idiomas

  Com a assinatura, você recebe as atualizações dos arquivos .DAT, não somente em diversas plataformas mas também nos idiomas de sua escolha.

- Suporte a HTTP no software de cliente

  O Enterprise SecureCast dá suporte a HTTP (Hypertext Transfer Protocol) para transmissão de arquivos através da sua barreira de proteção para os servidores do SecureCast.

NOTA: Considerações sobre a barreira de proteção: Se você tiver instalado uma barreira de proteção, use o HTTP. Caso contrário, use o UDP. Se estiver usando o software Firewall-1™ da Check Point, você notará que o BackWeb é um tipo de transmissão predefinida.

Configurando o Enterprise SecureCast

Para obter o cliente BackWeb, os usuários corporativos devem possuir primeiro um número de concessão (número de série da licença do produto) para inscrever-se no Enterprise SecureCast.

- Se você não tiver um número de concessão, entre em contato com o seu agente de vendas, o Revendedor com Valor Agregado (VAR - Value Added Reseller) ou com a Assistência ao Cliente da Network Associates, através do telefone (011) 550 51009, para obter assistência.
- Se você já for um cliente da Network Associates registrado e não souber o seu número de concessão, envie o formulário de solicitação de número de concessão online:

  http://www.nai.com/products/securecast/esc/grantreq.asp

OU

- Envie uma mensagem de correio eletrônico para o endereço adequado:

  ESCRegistration@nai.com (Estados Unidos)

  ESC-Registration-Europe@nai.com (Europa)

  ESC-Registration-Asia@nai.com (Ásia)

Siga estas etapas para configurar o Enterprise SecureCast:

1. Faça download do cliente BackWeb do Enterprise SecureCast (2MBaproximadamente). Este software de cliente é especialmente configurado para funcionar em ambiente corporativo, dando suporte a transmissão de arquivos HTTP.
2. Instale o software de cliente Enterprise SecureCast.

   Você receberá um Welcome InfoPak que lhe informa que a sua conexão ao canal Enterprise SecureCast está funcionando.
3. Inicie o processo de registro do canal digitando os dados sobre a sua empresa nas caixas de diálogo Informações sobre registro de cliente (que aparecerão no primeiro e no segundo InfoPak recebidos).

   Após clicar em **Avançar** na última caixa de diálogo de registro, a caixa de diálogo Status da atividade online acompanhará o status da transmissão de dados.

4. Quando o registro do usuário estiver completo, anote o seu número de registro, em seguida, clique em **Concluir**.

   O seu navegador da Web é iniciado mostrando um formulário de assinatura de contrato do produto.

5. Selecione o software, as plataformas e os idiomas nos quais você deseja receber as atualizações de arquivos e de versão.

6. Envie o formulário de assinatura de contrato do produto.

Usando o Enterprise SecureCast

Agora, você já está pronto para receber os Alertas de vírus e as atualizações de arquivos e de versão periódicos. Após alguns dias, serão enviados InfoPaks adicionais. Um InfoPak pode conter sons, animações, páginas da Web e muito mais. Ao receber um novo InfoPak do Enterprise SecureCast, ele aparecerá automaticamente como um objeto animado na sua área de trabalho até que seja aberto. Para abrir um InfoPak, basta clicar nele duas vezes.

Quando as atualizações estiverem no seu sistema, você deve distribuí-las para as estações de trabalho da rede. Os InfoPaks recebidos funcionam bem como pacotes de distribuição para o McAfee Enterprise (Me!) With Me!, você pode gerenciar atualizações de software, inventários, distribuição, medição de utilização e alerta centralizado. Entre em contato com o representante de vendas da Network Associates para obter mais informações sobre o Me!

Solução de problemas do Enterprise SecureCast

Problemas com o registro

Se você tentar se registrar em um período do dia de muito tráfego na Web, poderá ter que esperar enquanto o servidor processa a sua solicitação de registro. Caso receba a mensagem de erro “Erro 1105” ou “Erro do Banco de Dados: Não é possível conectar à origem de dados”, isto significa que há um problema com o banco de dados no servidor do SecureCast. Tente enviar o formulário novamente ou tente registrar-se posteriormente. Se continuar a ter problemas para fazer a assinatura do canal Enterprise SecureCast, entre em contato com o Suporte a Download da Network Associates (de segunda a sexta, das 8:00 às 20:00 Hora Central) pelo telefone 001 (972) 278-6100 para obter assistência.

Problemas com firewall

A maioria das firewalls que permitem tráfego de navegação na Web também lhe permitem receber os InfoPaks do SecureCast. Contudo, algumas firewalls podem causar problemas para as conexões com o servidor do SecureCast. Quando você preencher o formulário de registro e fizer download do software, inicialmente obterá por download um cliente SecureCast criado com o BackWeb versão 1.2. Como a versão 1.2 não dá suporte a determinados protocolos de comunicação, deve ser mostrado um erro semelhante a “não há conexão de rede” ao usá-la. Para corrigir esse problema, faça download do cliente SecureCast mais recente, que foi desenvolvido com o BackWeb versão 3.0.

NOTA: Você deve instalar o software de cliente que utiliza o BackWeb versão 3.0 sobre o cliente da versão 1.2 do BackWeb. *Não* desinstale primeiro a versão mais antiga. Este procedimento assegura que o novo cliente SecureCast reterá as preferências do seu canal.

Siga estas etapas para instalar e configurar o software de cliente SecureCast mais novo:

1. Instale o BackWeb versão 3.0 sobre o BackWeb versão 1.2.
2. Inicie o cliente SecureCast.
3. Para configurar o Método de Comunicação do cliente SecureCast com as suas informações de rede, escolha **Opções Globais** no menu **Preferências**.
4. Altere a configuração do modo como o BackWeb navega no servidor proxy, de **Polite Agent** para **HTTP**. Em seguida, clique em **Configuração do HTTP Proxy** e digite a informação solicitada sobre a sua rede.

   NOTA: A informação sobre o servidor proxy é específica para a sua rede. Se tiver mais perguntas a fazer, consulte o administrador de sistema.

Cancelando a assinatura do Enterprise SecureCast

Siga estas etapas para cancelar este serviço a qualquer momento:

1. Clique duas vezes no ícone do cliente SecureCast na área de status da barra de tarefas do Windows.
2. Clique com o botão direito no botão do canal **Empresarial**.

   Aparece um menu de atalho.
3. Clique em **Cancelar assinatura**, em seguida, clique em **OK** para confirmar.

Recursos de suporte

SecureCast

Se você tiver perguntas adicionais a fazer sobre o SecureCast, consulte o FAQ (perguntas mais freqüentes) do SecureCast:

http://www.nai.com/products/securecast/esc/enterprise_faq.asp

BackWeb

- Para obter uma descrição geral do BackWeb e dos InfoPaks, leia a Visão geral do BackWeb:

  http://www.nai.com/products/securecast/securedetail.asp

- Para obter um guia completo do BackWeb (incluindo conselhos adicionais para solução de problemas), coloque no seu marcador o Manual do Usuário do BackWeb:

  http://www.backweb.com/doc/version20/Client95/

OU

  faça download do arquivo .PDF:

  http://www.backweb.com/doc/version20/bwuser.pdf

- Para obter soluções para problemas sérios de operação do BackWeb, contate o Suporte a Download da Network Associates (de segunda a sexta, de 8:00 às 20:00 Hora Central) pelo telefone 001 (972) 278-6100.

Network Associates Serviços de suporte

B

A escolha do software antivírus e de segurança da Network Associates ajuda a assegurar que a tecnologia de informação crítica na qual você baseia-se funciona perfeitamente e com eficiência. Os benefícios do plano de suporte da Network Associates estende a proteção obtida com o seu software dando-lhe as instruções necessárias para instalar, monitorar, fazer a manutenção e atualizar a versão do sistema com a tecnologia mais recente da Network Associates. Com o plano de suporte projetado para atender as suas necessidades, você pode manter o sistema ou a rede funcionando de forma confiável em seu ambiente de computação por muitos meses ou anos.

Os planos de suporte da Network Associates são oferecidos em duas categorias. Se você for um cliente corporativo, poderá escolher entre três níveis de suporte prolongado no programa PrimeSupport da Network Associates. Se tiver adquirido uma versão para o varejo de um produto da Network Associates, poderá escolher um plano dirigido às suas necessidades no plano Suporte Pessoal.

Opções do PrimeSupport para clientes corporativos

O programa PrimeSupport da Network Associates oferece as opções Básico, Estendido ou Permanente. Cada opção apresenta diversos recursos que fornecem suporte imediato e econômico dirigido para atender as suas necessidades.

Opção PrimeSupport Básico

A opção PrimeSupport Básico lhe oferece acesso telefônico aos membros experientes da equipe de suporte técnico da Network Associates para obter assistência ao produto. Se você adquiriu o software da Network Associates com uma licença de assinatura, recebeu a opção PrimeSupport Básico como parte do pacote de dois anos a partir da data de compra. Se tiver adquirido o produto da Network Associates com uma licença permanente, poderá renovar o seu plano de PrimeSupport Básico após o pagamento de uma taxa anual.

A opção PrimeSupport Básico inclui estes recursos:

- Acesso telefônico ao suporte técnico de segunda a sexta, das 8:00 às 20:00, Horário Central dos EUA.
- Acesso 24 horas irrestrito às informações do suporte técnico, através do site da Web da Network Associates.
- Atualizações dos arquivos de dados e atualizações de versão através do site da Web da Network Associates.

Opção PrimeSupport Estendido

O PrimeSupport Estendido lhe oferece suporte personalizado e dinâmico de um engenheiro de suporte técnico específico. Estará à sua disposição um profissional de suporte que está familiarizado com a distribuição e histórico de suporte do seu produto da Network Associates, e que entrará em contato em intervalos que você determina para verificar se você sabe usar e fazer a manutenção dos produtos da Network Associates. Telefonando com antecedência, o representante do PrimeSupport Estendido poderá ajudá-lo a evitar problemas antes que ocorram. Se, contudo, houver um caso de emergência, o PrimeSupport Estendido estabelecerá um prazo de resposta para assegurar que a ajuda está a caminho. O PrimeSupport Estendido pode ser adquirido por um ano a partir da compra de um produto da Network Associates com uma licença de assinatura ou permanente.

O PrimeSupport Estendido inclui estes recursos:

- Acesso a um engenheiro de suporte específico.
- Contatos de suporte dinâmico através de telefone ou correio eletrônico com o seu engenheiro de suporte específico, a intervalos determinados por você.
- Prazos de resposta: o seu engenheiro de suporte responderá em uma hora ao pager, em quatro horas ao correio de voz e em 12 horas ao correio eletrônico.
- Acesso telefônico ao suporte técnico de segunda a sexta, de 7:00 às 19:00. Hora Central.
- Acesso irrestrito 24 horas às informações do suporte técnico através do site da web da Network Associates.
- Atualizações dos arquivos de dados e atualizações de versão do produto, através do site da Web da Network Associates.
- Possibilidade de designar até cinco pessoas em sua organização como contatos do cliente.

PrimeSupport Permanente

O PrimeSupport Permanente lhe oferece suporte dinâmico e personalizado, 24 horas, para os produtos da Network Associates distribuídos nos sistemas de informação sobre negócios mais críticos. O PrimeSupport Permanente coloca à sua disposição os recursos do PrimeSupport Estendido durante 24 horas, sete dias na semana, com o menor tempo de resposta. Você pode adquirir o PrimeSupport Permanente anual ao comprar um produto da Network Associates, com uma licença de assinante ou permanente.

O PrimeSupport Permanente inclui estes recursos:

- Acesso a um engenheiro de suporte específico.
- Contatos de suporte dinâmico através de telefone ou correio eletrônico com o seu engenheiro de suporte específico, a intervalos determinados por você.
- Prazos de resposta: o seu engenheiro de suporte responderá em meia hora ao pager, em uma hora ao correio de voz e em quatro horas ao correio eletrônico.
- Acesso telefônico ao suporte técnico 24 horas, sete dias na semana.
- Acesso irrestrito 24 horas às informações do suporte técnico através do site da web da Network Associates.
- Atualizações dos arquivos de dados e atualizações de versão do produto, através do site da Web da Network Associates.
- Possibilidade de designar até dez pessoas em sua organização como contatos do cliente.

Tabela B-1. PrimeSupport Imediato

Recurso	Básico	Estendido	Permanente
Suporte técnico pelo telefone	Segunda a Sexta, de 8:00 às 20:00.	Segunda a Sexta, de 7:00 às 19:00.	de 7:00 às 19:00. 24 horas, 7 dias na semana
Suporte técnico no site da Web	Sim	Sim	Sim
Atualizações do software	Sim	Sim	Sim
Engenheiro de suporte específico	—	Sim	Sim

Tabela B-1. PrimeSupport Imediato

Recurso	Básico	Estendido	Permanente
Contato de suporte dinâmico	—	Sim	Sim
Contatos de suporte designados	—	5	10
Prazo de resposta	—	Pager: 1 hora Correio de voz: 4 horas Correio eletrônico: 12 horas	Pager: 30 min. Correio de voz: 1 hora Correio eletrônico: 4 horas

Pedindo o PrimeSupport

Para pedir o PrimeSupport Básico, Estendido ou Permanente para os produtos da Network Associates: Entre em contato com o seu representante de vendas, ou

- Entre em contato com o seu representante de vendas ou
- Ligue para os Serviços de Suporte da Network Associates no telefone 1-800-988-5737 ou 00-1-650-473-2000, de segunda a sexta , de 6:00 às 17:00. Hora do Pacífico.

NOTA: O programa PrimeSupport descrito neste guia está disponível somente na América do Norte. Para conhecer as opções do PrimeSupport disponíveis fora da América do Norte, entre em contato com o escritório de vendas regional. As informações sobre contato aparecem no início deste guia.

Serviços de suporte para clientes do varejo

Se você adquirir o seu produto da Network Associates através de um varejista local ou do site da web da Network Associates, também receberá alguns serviços de suporte como parte de sua compra. Este nível específico de suporte incluído depende do produto adquirido. Os exemplos dos serviços recebidos incluem:

- Atualizações gratuitas dos arquivos (.DAT) de dados durante a vida de seu produto através do site da web da Network Associates, o recurso AutoUpdate para o seu produto ou o serviço SecureCast (veja o Apêndice A, “Usando o SecureCast para atualizar o software” para obter mais detalhes). Você também pode atualizar os arquivos de dados usando o navegador da web para visitar

  http://www.nai.com/download/updates/updates.asp

- Atualizações de versão gratuitas do programa (arquivo executável) durante um ano através do site da web da Network Associates, o recurso AutoUpdate para o seu produto ou o serviço SecureCast (veja o Apêndice A, “Usando o SecureCast para atualizar o software” para obter mais detalhes). Se você adquirir uma versão especial do produto da Network Associates, receberá atualizações de versão do produto gratuitas durante dois anos. A atualização de versão do software também pode ser feita usando o seu navegador da Web para visitar o site:

  http://www.nai.com/download/upgrades/upgrades.asp

- Acesso gratuito 24 horas, sete dias na semana a suporte online ou eletrônico via sistema de voz ou fax, ou site da Web da Network Associates e através de outros serviços eletrônicos, como America Online e CompuServe.

  Para entrar em contato com os serviços eletrônicos da Network Associates escolha uma destas opções:

  – Sistema de voz e fax automático: (408) 988-3034
  – Site da Web da Network Associates: http://www.nai.com
  – CompuServe: GO NAI
  – America Online: palavra-chave MCAFEE

- Noventa dias de suporte de cortesia fornecido por um técnico de suporte da Network Associates durante horário comercial, de segunda a sexta, das 8:00 às 18:00. Hora Central dos EUA.

Após expirar o período de suporte de cortesia, você poderá beneficiar-se das várias opções de suporte pessoal dirigidas para atender às suas necessidades. Entre em contato com a Assistência ao Cliente da Network Associates através do telefone 00 1 (972) 278-6100 para conhecer as opções disponíveis, ou visite o site da Web da Network Associates em:

http://www.nai.com/services/support/support.asp.

Treinamento e Consultoria da Network Associates

A Network Associates fornece consultoria profissional de alto nível e treinamento completo que podem ajudá-lo a maximizar a segurança e o desempenho da sua rede de investimentos através do programa Total Service Solutions da Network Associates.

Serviços de consultoria profissional

Os Serviços de consultoria profissional da Network Associates estão prontos para dar assistência em todos os estágios do desenvolvimento da sua rede, do planejamento e desenho à implementação, com gerenciamento contínuo. Os consultores da Network Associates oferecem recursos suplementares profissionais e perspectiva independente para resolver os seus problemas. Você obterá ajuda para integração dos produtos da Network Associates ao seu ambiente, bem como assistência para a solução de problemas ou ajuda para estabelecer as bases do desempenho de uma rede. Os consultores da Network Associates também desenvolvem e sugerem soluções personalizadas para ajudá-lo a atingir os objetivos de seus projetos — de implementações extensas e em larga escala à solução de pequenos problemas.

Serviços educacionais completos

Os Serviços educacionais completos da Network Associates desenvolvem e aprimoram as habilidades de todos os profissionais de rede através de instruções práticas que podem ser utilizadas imediatamente em seu trabalho. O currículo da tecnologia Serviços educacionais completos é dirigida para o gerenciamento do desempenho e das falhas de rede, além de abranger a solução de problemas em todos os níveis. A Network Associates oferece também treinamento de produto modular para que você possa compreender os recursos e funcionalidade do seu novo software.

A inscrição para os cursos dos Serviços educacionais completos está aberta o ano inteiro nos centros educacionais da Network Associates, ou você poderá aprender nos cursos personalizados, implementados em seu local de trabalho. Todos os cursos seguem etapas educacionais em uma linha de aprendizado que o leva ao mais alto nível técnico. A Network Associates é membro fundador do consórcio Certified Network Expert (CNX).

Para obter mais informações sobre esses programas, entre em contato com o seu representante de vendas ou ligue para Total Service Solutions no telefone 00 1-800-395-3151.

Compreendendo o formato de arquivo .VSC

C

Salvando as configurações das tarefas do VirusScan

Quando você escolhe as opções de configuração para o VirusScan, o programa salva as definições no arquivo DEFAULT.VSC, que se encontra no diretório de programa do VirusScan. O DEFAULT.VSC é um arquivo de texto de configuração que descreve as definições do VirusScan. O arquivo é formatado de maneira semelhante aos arquivos .INI do Windows. Esse arquivo pode ser editado diretamente para alterar as opções nele gravadas — basta abrir o arquivo com um editor de texto, como o Bloco de Notas do Windows. Se você tiver protegido por senha as definições do VirusScan, o programa criptografará o DEFAULT.VSC para impedir adulterações — é necessário remover a proteção para editar o arquivo.

Cada variável no arquivo tem um nome seguido por um sinal de igual (=) e um valor. Os valores correspondem às definições selecionadas durante a configuração do VirusScan. As variáveis são organizadas em oito grupos que aparecem abaixo de seus cabeçalhos no DEFAULT.VSC. As tabelas nas páginas seguintes apresentam cada variável com seus valores padrão e possível.

NOTA: Às variáveis booleanas podem ser atribuídos apenas 0 e 1 como valores possíveis. O valor 0 instrui o VirusScan a desativar a definição, o valor 1 ativa-a.

Você pode distribuir cópias do arquivo DEFAULT.VSC editado para outros usuários do VirusScan que utilizem computadores diferentes, substituir os arquivos DEFAULT.VSC existentes e assim copiar as definições do VirusScan para serem executadas por outro usuário. O VirusScan também permite salvar os arquivos .VSC com qualquer nome escolhido. Se esses arquivos forem distribuídos para outros usuários, eles precisarão localizá-los e clicar neles duas vezes para iniciar o VirusScan com as opções criptografadas.

A Network Associates também fornece o ISeamless, uma ferramenta de distribuição e configuração com recursos completos que permite controlar totalmente os arquivos de configuração do VirusScan, inclusive o DEFAULT.VSH, DEFAULT.VSC, UPGRADE.INI, UPDATE.INI e quaisquer outros arquivos desse tipo criados e salvados. Para saber mais sobre o ISeamless e as outras ferramentas administrativas da Network Associates, consulte o seu representante de vendas ou ligue para a Assistência ao Cliente da Network Associates.

ScanOptions (Opções de varredura)

Variável	Descrição
bAutoStart	Tipo: Booleana (0/1) Instrui o VirusScan para iniciar sua execução automaticamente quando for ativado Valor padrão: 0
bAutoExit	Tipo: Booleana (0/1) Instrui o VirusScan para sair automaticamente quando terminar a varredura, quando nenhum vírus for encontrado. Valor padrão: 0
bAlwaysExit	Tipo: Booleana (0/1) Instrui o VirusScan para sair automaticamente ao terminar a varredura, mesmo se forem encontrados vírus. Valor padrão: 0
bSkipMemoryScan	Tipo: Booleana (0/1) Instrui o VirusScan a ignorar a varredura da memória Valor padrão: 0
bSkipBootScan	Tipo: Booleana (0/1) Instrui o VirusScan a ignorar a varredura do setor de inicialização. Valor padrão: 0
bSkipSplash	Tipo: Booleana (0/1) Instrui o VirusScan a ignorar a exibição da tela do logotipo do produto do VirusScan ao iniciá-lo. Valor padrão: 0

DetectionOptions (Opções de detecção)

Variável	Descrição
bScanAllFiles	Tipo: Booleana (0/1) Instrui o VirusScan a examinar todos os tipos de arquivos. Valor padrão: 0
bScanCompressed	Tipo: Booleana (0/1) Instrui o VirusScan a examinar os arquivos compactados. Valor padrão: 1
szProgramExtensions	Tipo: Seqüência de caracteres Especifica quais extensões de arquivo o VirusScan examinará. Valor padrão: EXE COM DO? XL?
szDefaultProgram Extensions	Tipo: Seqüência de caracteres Especifica o valor padrão para szProgramExtensions Valor padrão: EXE COM DO? XL?

AlertOptions (Opções de ação)

Variável	Descrição
bNetworkAlert	Tipo: Booleana (0/1) Instrui o VirusScan a enviar um arquivo (.ALR) de alerta para um caminho de rede, que esteja sendo monitorado pelo Alerta Centralizado do NetShield, quando um vírus for encontrado. Valor padrão: 0
bSoundAlert	Tipo: Booleana (0/1) Instrui o VirusScan a emitir um alerta audível quando um vírus for detectado. Valor padrão: 1
szNetworkAlertPath	Tipo: Seqüência de caracteres Especifica o caminho de alerta de rede que está sendo monitorado pelo Alerta Centralizado do NetShield. A pasta indicada por esse caminho deve conter o arquivo de Alerta Centralizado, CENTALRT.TXT Valor padrão: Nenhum

ActionOptions (Opções de ação)

Variável	Descrição
bDisplayMessage	Tipo: Booleana (0/1) Instrui o VirusScan a exibir uma mensagem ao detectar um vírus. Valor padrão: 0
ScanAction	Tipo: Número inteiro (0-5) Instrui o VirusScan a realizar a ação especificada quando um vírus for detectado Valores possíveis: 0 - Solicita ação 1 – Move automaticamente 2 – Limpa automaticamente 3 – Exclui automaticamente 4 – Continua Valor padrão: 0
bButtonClean	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Limpar se ScanAction=0. Valor padrão: 1
bButtonDelete	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Excluir se ScanAction=0. Valor padrão: 1
bButtonExclude	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Eliminar se ScanAction=0. Valor padrão: 1
bButtonMove	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Mover se ScanAction=0. Valor padrão: 1
bButtonContinue	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Continuar se ScanAction=0. Valor padrão: 1

Variável	Descrição
bButtonStop	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Parar se ScanAction=0. Valor padrão: 1
szMoveToFolder	Tipo: Seqüência de caracteres Indica para onde os arquivos infectados devem ser movidos Valor padrão: \Infectado
szCustomMessage	Tipo: Seqüência de caracteres Indica o texto da mensagem que deve ser exibido ao ser detectado um vírus. Valor padrão: Possível Vírus Detectado

ReportOptions (Opções de relatório)

Variável	Descrição
bLogToFile	Tipo: Booleana (0/1) Instrui o VirusScan a registrar a atividade de varredura em um arquivo. Valor padrão: 1
bLimitSize	Tipo: Booleana (0/1) Instrui o VirusScan a limitar o tamanho do arquivo de registro. Valor padrão: 1
uMaxKilobytes	Tipo: Número inteiro (10-999) Especifica o tamanho máximo do arquivo de registro em quilobytes Valor padrão: 10
bLogDetection	Tipo: Booleana (0/1) Instrui o VirusScan a registrar a detecção de vírus. Valor padrão: 1
bLogClean	Tipo: Booleana (0/1) Instrui o VirusScan a registrar a limpeza de vírus. Valor padrão: 1

Variável	Descrição
bLogDelete	Tipo: Booleana (0/1) Instrui o VirusScan a registrar as exclusões de arquivos. Valor padrão: 1
bLogMove	Tipo: Booleana (0/1) Instrui o VirusScan a registrar os deslocamentos de arquivos. Valor padrão: 1
bLogSettings	Tipo: Booleana (0/1) Instrui o VirusScan a registrar as configurações da sessão. Valor padrão: 1
bLogSummary	Tipo: Booleana (0/1) Instrui o VirusScan a registrar os resumos de sessões. Valor padrão: 1
bLogDateTime	Tipo: Booleana (0/1) Instrui o VirusScan a registrar a data e a hora da atividade de varredura. Valor padrão: 1
bLogUserName	Tipo: Booleana (0/1) Instrui o VirusScan a registrar o nome do usuário. Valor padrão: 1
szLogFileName	Tipo: Seqüência de caracteres Especifica o caminho para o arquivo de registro. Valor padrão: C:\Program Files\Network Associates\McAfee Viruscan\VSCLOG.TXT

ScanItems (Itens de varredura)

Variável	Descrição
ScanItem_x, onde x é um índice com base zero	Tipo: Seqüência de caracteres Instrui o VirusScan a examinar o item. Valor padrão: `C:|1 *` * A seqüência é separada em campos por uma barra vertical (|): Campo 1 - Caminho do item a ser examinado. Campo 2 - Booleano (1/0) Valores possíveis: 1 - Instrui o VirusScan a examinar as subpastas do item. 2 - Instrui o VirusScan a não examinar as subpastas do item.

SecurityOptions (Opções de segurança)

Variável	Descrição
szPasswordProtect	Tipo: Seqüência de caracteres Esta variável não pode ser configurada pelo usuário Valor padrão: 0
szPasswordCRC	Tipo: Seqüência de caracteres Esta variável não pode ser configurada pelo usuário Valor padrão: 0
szSerialNumber	Tipo: Seqüência de caracteres Esta variável não pode ser configurada pelo usuário Valor padrão: 0

ExcludedItems (Itens excluídos)

Variável	Descrição
NumExcludeItems	Tipo: Número inteiro (0-n) Define o número de itens eliminados da varredura. Valor padrão: 1
ExcludedItem_x, onde x é um índice de base zero	Tipo: Seqüência de caracteres Cadeia de caracteres Instrui o VirusScan a eliminar o item da varredura. Valor padrão: `\Recycled|*.*|1|1 *` * A seqüência é separada em campos por uma barra vertical (|): Campo 1 - Parte relativa à pasta do item a ser excluído. Deixar em branco para um único arquivo em qualquer lugar do sistema. Campo 2 - Parte relativa ao arquivo do item a ser excluído. Deixe em branco se uma pasta for excluída sem um nome de arquivo. Campo 3 - Número inteiro (1-3) Valores possíveis: 1 - Elimina da varredura de arquivos. 2 - Excluir da varredura de registro de inicialização 3 - Elimina da varredura do registro de inicialização e de arquivos. Campo 4 - Booleano (1/0) Valores possíveis: 1 - Instrui o VirusScan a eliminar as subpastas do item excluído. 2 - Instrui o VirusScan a não eliminar as subpastas.

Compreendendo o formato .VSH de arquivo

Salvando as opções de configuração do VShield

Quando você escolhe as opções de configuração para o VShield, o VirusScan salva essas definições no arquivo DEFAULT.VSH, que se encontra no diretório de programa do VirusScan. O DEFAULT.VSH é um arquivo de texto de configuração que descreve as definições do VShield. O arquivo é formatado de modo semelhante aos arquivos .INI do Windows. Pode ser editado diretamente para alterar as opções nele gravadas — basta abrir o arquivo com um editor de texto, como o Bloco de Notas do Windows. Se as definições do VShield estiverem protegidas por senha, o VirusScan criptografará o DEFAULT.VSH para impedir adulterações — é necessário remover a proteção por senha para poder editar o arquivo.

Cada variável no arquivo tem um nome seguido por um sinal de igual (=) e um valor. Os valores correspondem, às definições selecionadas durante a configuração do VShield. As variáveis são organizadas em 24 grupos que aparecem abaixo de seus cabeçalhos no DEFAULT.VSH. A maioria desses cabeçalhos correspondem a um módulo VShield. As tabelas nas páginas seguintes mostram cada variável com seus valores padrão e possível.

NOTA: Às variáveis booleanas podem ser atribuídos apenas 0 e 1 como valores possíveis. Um valor 0 instrui o VShield a desativar a definição, o valor 1 ativa-a.

Você pode distribuir cópias do arquivo DEFAULT.VSH editado para outros usuários do VShield que utilizem computadores diferentes, substituir os arquivos DEFAULT.VSH e assim copiar as definições do VShield para serem executadas por outro usuário. A Network Associates também fornece o ISeamless, uma ferramenta de distribuição e configuração com recursos completos que permitem a você controlar totalmente os arquivos de configuração do VirusScan, inclusive o DEFAULT.VSH, DEFAULT.VSC, UPGRADE.INI, UPDATE.INI e quaisquer outros arquivos desse tipo criados e salvados.

Para saber mais sobre o ISeamless e as outras ferramentas administrativas da Network Associates, consulte o seu representante de vendas ou ligue para a Assistência ao Cliente da Network Associates.

Módulo Varredura do Sistema

Geral (General)

Variável	Descrição
bEnabled	Tipo: Booleana (1/0) Ativa a Varredura do Sistema Valor padrão: 1
bCanBeDisabled	Tipo: Booleana (1/0) Define se o VShield pode ser desativado Valor padrão: 1
bShowTaskbarIcon	Tipo: Booleana (1/0) Define se a barra de tarefas do VShield é exibida Valor padrão: 1

DetectionOptions (Opções de detecção)

Variável	Descrição
bProgFileHeurisitcs	Tipo: Booleana (1/0) Instrui o VShield a examinar heuristicamente os arquivos de programa Valor padrão: 0
bMacroHeuristics	Tipo: Booleana (1/0) Instrui o VShield a examinar as macros heuristicamente Valor padrão: 0
bDetectTrojans	Tipo: Booleana (1/0) Instrui o VShield a examinar os vírus do tipo cavalo de Tróia Valor padrão: 1
bDetectJoke	Tipo: Booleana (1/0) Instrui o VShield a examinar vírus do tipo Joke Valor padrão: 1
bDetectCorrupted	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos danificados Valor padrão: 0

Variável	Descrição
bDetectMaybe	Tipo: Booleana (1/0) Instrui o VShield a examinar as variantes de vírus conhecidos Valor padrão: 1
bRemoveAllMacros	Tipo: Booleana (1/0) Instrui o VShield a excluir todas as macros dos arquivos infectados Valor padrão: 0
bScanOnExecute	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando forem executados Valor padrão: 1
bScanOnOpen	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando forem abertos Valor padrão: 1
bScanOnCreate	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando forem criados Valor padrão: 1
bScanOnRename	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando forem renomeados Valor padrão: 1
bScanOnShutdown	Tipo: Booleana (1/0) Instrui o VShield a examinar o setor de inicialização da unidade A quando o sistema é fechado Valor padrão: 1
bScanOnBootAccess	Tipo: Booleana (1/0) Instrui o VShield a examinar o registro de inicialização de um disquete que acabou de ser inserido em uma unidade logo antes do acesso à unidade de disco. Valor padrão: 1
bScanAllFiles	Tipo: Booleana (1/0) Instrui o VShield a examinar todos os arquivos, com qualquer extensão. Valor padrão: 0

Variável	Descrição
bScanCompressed	Tipo: Booleana (1/0) Instrui o programa a examinar os arquivos compactados Valor padrão: 1
szProgramExtensions	Tipo: Seqüência de caracteres Define as extensões dos arquivos a serem examinados Valor padrão: EXE COM DO? XL? MD?, SYS BIN RTF OBD (O ? é um curinga)
szDefaultProgram Extensões	Tipo: Seqüência de caracteres Define as extensões de programa padrão a serem utilizadas durante a configuração da varredura Valor padrão: EXE COM DO? XL? MD?, SYS BIN RTF OBD (O ? é um curinga)

AlertOptions (Opções de ação)

Variável	Descrição
bDMIAlert	Tipo: Booleana (1/0) Ativa o Alerta Desktop Management Interface Valor padrão: 0
bSoundAlert	Tipo: Booleana (1/0) Ativa um sinal sonoro audível quando um vírus for detectado Valor padrão: 1
bNetworkAlert	Tipo: Booleana (1/0) Ativa Alerta Centralizado Valor padrão: 0
szNetworkAlertPath	Tipo: Seqüência de caracteres Especifica a pasta Alerta Centralizado do servidor Valor padrão: Nenhum

ActionOptions (Opções de ação)

Variável	Descrição
bDisplayMessage	Tipo: Booleana (1/0) Define se uma mensagem personalizada deve ser exibida na caixa de diálogo Solicitar ação, quando um vírus for detectado Valor padrão: 0
uVshieldAction	Tipo: Número inteiro (1-5) Instrui o VShield a realizar a ação especificada quando um vírus é detectado Valores possíveis: 1 – Solicitar ação 2 – Mover arquivos infectados automaticamente 3 - Limpar os arquivos infectados automaticamente (Negar acesso se os arquivos não puderem ser limpos) 4 – Excluir arquivos infectados automaticamente 5 - Negar acesso para arquivos infectados e continuar Valor padrão: 1
bButtonClean	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário uma opção de limpeza de arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonDelete	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de excluir o arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonExclude	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de eliminar um arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonContinue	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de continuar com o evento interrompido, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 0

Variável	Descrição
bButtonStop	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de negar acesso ao arquivo infectado, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
szMoveToFolder	Tipo: Seqüência de caracteres Define a pasta para a qual os arquivos infectados devem ser movidos Valor padrão: \Infectado
szCustomMessage	Tipo: Seqüência de caracteres Define a mensagem personalizada a ser exibida quando um vírus for detectado, se a ação estiver configurada como Solicitar ação Valor padrão: Nenhum

ReportOptions (Opções de relatório)

Variável	Descrição
bLogToFile	Tipo: Booleana (1/0) Define se os resultados devem ser inseridos no arquivo de registro Valor padrão: 1
bLimitSize	Tipo: Booleana (1/0) Define se o tamanho do arquivo de registro deve ser limitado Valor padrão: 1
uMaxKilobytes	Tipo: Número inteiro (10-999) Define o tamanho máximo do arquivo de registro, em quilobytes Valor padrão: 100
bLogDetection	Tipo: Booleana (1/0) Instrui o VShield a registrar os nomes dos vírus detectados Valor padrão: 1
bLogClean	Tipo: Booleana (1/0) Define se os resultados da limpeza devem ser registrados Valor padrão: 1

Variável	Descrição
bLogDelete	Tipo: Booleana (1/0) Define se as operações de exclusão do arquivo infectado devem ser registradas Valor padrão: 1
bLogMove	Tipo: Booleana (1/0) Define se as operações de movimentação do arquivo devem ser registradas Valor padrão: 1
bLogSettings	Tipo: Booleana (1/0) Instrui o VShield a gravar um registro das definições utilizadas durante a sessão de varredura que precedeu o fechamento do sistema ou o descarregamento do VShield Valor padrão: 1
bLogSummary	Tipo: Booleana (1/0) Instrui o VShield a gravar um resumo de suas descobertas e ações durante a sessão de varredura que precedeu o fechamento do sistema, ou o descarregamento do VShield Valor padrão: 1
bLogDateTime	Tipo: Booleana (1/0) Define se a hora e data de um evento devem ser registradas Valor padrão: 1
bLogUserName	Tipo: Booleana (1/0) Define se o nome do usuário deve ser registrado Valor padrão: 1
szLogFileName	Tipo: Seqüência de caracteres Define o nome do arquivo de registro Valor padrão: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

ExclusionOptions (Opções de exclusão)

Variável	Descrição
szExclusionsFileName	Tipo: Seqüência de caracteres Valor padrão: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

ExcludedItems (Itens excluídos)

Variável	Descrição
NumExcludedItems	Tipo: Número inteiro (0-n) Define o número de itens excluídos da varredura ao acessar Valor padrão: 1
ExcludedItem_x, onde x é um índice de base zero	Tipo: Seqüência de caracteres Seqüência de caracteres Instrui o VShield a eliminar o item da varredura ao acessar Valor padrão: \Reciclado|*.*|1|1 * * A seqüência é separada em campos por uma barra vertical (|): Campo 1 - Parte relativa à pasta do item a ser excluído. Deixar em branco para um único arquivo em qualquer lugar do sistema. Campo 2 - Parte relativa ao arquivo do item a ser excluído. Deixar em branco se uma pasta for excluída sem um nome de arquivo. Campo 3 - Número inteiro (1-3) Valores possíveis: 1 - Excluir da varredura de arquivo 2 - Excluir da varredura de registro de inicialização 3 - Excluir da varredura de arquivo e de registro de inicialização Campo 4 - Booleano (1/0) Valores possíveis: 1 - Instrui o VShield a excluir as subpastas do item excluído 0 - Instrui o VShield a não excluir as subpastas

Módulo Varredura de Correio Eletrônico

EMailGeneralOptions

Variável	Descrição
bMailType	Tipo: Booleana (1/0) Define o tipo de servidor de correio eletrônico, MAPI ou cc:Mail. Valor padrão: 1 (MAPI)
bCanBeDisabled	Tipo: Booleana (1/0) Impede a desativação da varredura de correio eletrônico Valor padrão: 1
bEnabled	Tipo: Booleana (1/0) Ativa a varredura de correio eletrônico Valor padrão: 0
bEnabledDummy=0	Tipo: Booleana (1/0) Seleciona automaticamente o Correio da Internet na página de propriedades Varredura de Correio Eletrônico, quando a Varredura de Download estiver ativada Valor padrão: 0

EMailDetectionOptions

Variável	Descrição
bScanAllMails	Tipo: Booleana (1/0) Instrui o VShield a examinar todo o novo correio Valor padrão: 0
bScanInternetMail	Tipo: Booleana (1/0) Instrui o VShield a examinar o Correio da Internet Valor padrão: 0
bScanAllFiles	Tipo: Booleana (1/0) Instrui o VShield a examinar todos os arquivos Valor padrão: 0
bScanCompressed	Tipo: Booleana (1/0) Instrui o VShield a incluir os arquivos compactados na varredura Valor padrão: 1

Variável	Descrição
szProgramExtensions	Tipo: Seqüência de caracteres Define as extensões de arquivos a serem examinados Valor padrão: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (O ? é um curinga)
szDefaultProgram Extensões	Tipo: Seqüência de caracteres Define as extensões de programa padrão a serem utilizadas durante a configuração da varredura Valor padrão: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (O ? é um curinga)
uPollInterval	Tipo: Número inteiro (60-999) Define o intervalo, em segundos, das verificações de novo correio recebido via cc:Mail Valor padrão: 60
bDetectTrojans	Tipo: Booleana (1/0) Instrui o VShield a examinar vírus do tipo cavalo de Tróia Valor padrão: 1
bDetectJoke	Tipo: Booleana (1/0) Instrui o VShield a examinar vírus do tipo Joke Valor padrão: 1
bDetectCorrupted	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos danificados Valor padrão: 0
bDetectMaybe	Tipo: Booleana (1/0) Instrui o VShield a examinar as variantes de vírus conhecidos Valor padrão: 1
bProgFileHeuristics	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos de programa heuristicamente Valor padrão: 0
bMacroHeuristics	Tipo: Booleana (1/0) Instrui o VShield a examinar as macros heuristicamente Valor padrão: 0

EMailActionOptions

Variável	Descrição
szMoveFolder	Tipo: Seqüência de caracteres Define a pasta para a qual os anexos de correio eletrônico infectados devem ser movidos Valor padrão: \Infectado
CC_szMoveFolder	Tipo: Seqüência de caracteres Define a pasta para a qual os anexos de correio eletrônico do cc:Mail devem ser movidos Valor padrão: \Infectado
bDisplayMessage	Tipo: Booleana (1/0) Define se uma mensagem personalizada deve ser exibida na caixa de diálogo Solicitar ação, quando um vírus for detectado Valor padrão: 0
uScanAction	Tipo: Número inteiro (0/3) Instrui o VShield a realizar a ação especificada quando um vírus é detectado Valores possíveis: 0 – Solicitar ação 1 – Mover arquivos infectados automaticamente 2 – Excluir arquivos infectados automaticamente 3 - Continuar a varredura
bButtonDelete	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de excluir o arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonExclude	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de eliminar um arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 0
bButtonMove	Tipo: Booleana (1/0) Instrui o VirusScan a fornecer ao usuário a opção de mover o arquivo infectado, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1

Variável	Descrição
bButtonContinue	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de continuar com o evento interrompido, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonStop	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de negar acesso ao arquivo infectado, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 0

EMailAlertOptions

Variável	Descrição
bDMIAlert	Tipo: Booleana (1/0) Ativa o Alerta Desktop Management Interface Valor padrão: 0
bNetworkAlert	Tipo: Booleana (1/0) Ativa Alerta Centralizado Valor padrão: 0
szNetworkAlertPath	Tipo: Seqüência de caracteres Especifica uma pasta Alerta Centralizado do servidor Valor padrão: Nenhum
szCustomMessage	Tipo: Seqüência de caracteres Define a mensagem personalizada a ser exibida quando um vírus for detectado, se a ação estiver configurada como Solicitar ação Valor padrão: McAfee VShield: Encontrado vírus no anexo!
bReturnMail	Tipo: Booleana (1/0) Instrui o VShield a notificar o remetente do correio eletrônico infectado, recebido via cliente MAPI Valor padrão: 0
szReturnCc	Tipo: Seqüência de caracteres Identifica o(s) destinatário(s) da cópia da notificação para o remetente do correio eletrônico infectado, recebido via cliente MAPI Valor padrão: Nenhum

Variável	Descrição
szReturnSubject	Tipo: Seqüência de caracteres Permite a inserção de texto no campo Assunto na notificação ao remetente do correio eletrônico infectado, recebido via cliente MAPI Valor padrão: Nenhum
szReturnBody	Tipo: Seqüência de caracteres Permite a inclusão do texto da mensagem na notificação para o remetente do correio eletrônico infectado, recebido via cliente MAPI Valor padrão: Nenhum
bSendMailToUser	Tipo: Booleana (1/0) Instrui o VShield a notificar outros usuários de correio eletrônico infectado, recebido via cliente MAPI Valor padrão: 0
szSendTo	Tipo: Seqüência de caracteres Identifica outros usuários que deveriam receber notificação de correio eletrônico infectado, recebido via cliente MAPI Valor padrão: Nenhum
szSendCc	Tipo: Seqüência de caracteres Identifica as pessoas que deveriam receber cópias da notificação para outros usuários sobre correio eletrônico infectado, recebido via cliente MAPI Valor padrão: Nenhum
szSendSubject	Tipo: Seqüência de caracteres Permite a inserção de texto no campo Assunto na notificação para outros usuários de correio eletrônico infectado, recebido via cliente MAPI Valor padrão: Nenhum
szSendBody	Tipo: Seqüência de caracteres Permite a inclusão do texto da mensagem na notificação para outros usuários de correio eletrônico infectado, recebido via cliente MAPI Valor padrão: Nenhum
CC_bReturnMail	Tipo: Booleana (1/0) Instrui o VShield a notificar o remetente do correio eletrônico infectado, recebido via cc:Mail Valor padrão: 0

Variável	Descrição
CC_bSendMailToUser	Tipo: Booleana (1/0) Instrui o VShield a notificar outros usuários de correio eletrônico infectado, recebido via cc:Mail Valor padrão: 0
CC_szReturnCc	Tipo: Seqüência de caracteres Identifica o(s) destinatário(s) da cópia da notificação ao remetente do correio eletrônico infectado, recebido via cc:Mail Valor padrão: Nenhum
CC_szReturnSubject	Tipo: Seqüência de caracteres Permite a inserção de texto no campo Assunto para notificar o remetente de correio eletrônico infectado, recebido via cc:Mail Valor padrão: Nenhum
CC_szReturnBody	Tipo: Seqüência de caracteres Permite a inclusão do texto da mensagem na notificação ao remetente do correio eletrônico infectado, recebido via cc:Mail Valor padrão: Nenhum
CC_szSendTo	Tipo: Seqüência de caracteres Identifica os outros usuários que deveriam receber a notificação sobre correio eletrônico infectado, recebido via cc:Mail Valor padrão: Nenhum
CC_szSendCc	Tipo: Seqüência de caracteres Identifica as pessoas que deveriam receber cópias da notificação para outros usuários sobre correio eletrônico infectado, recebido via cc:Mail Valor padrão: Nenhum
CC_szSendSubject	Tipo: Seqüência de caracteres Permite a inserção de texto no campo Assunto para notificar outros usuários sobre correio eletrônico infectado, recebido via cc:Mail Valor padrão: Nenhum
CC_szSendBody	Tipo: Seqüência de caracteres Permite a inclusão do texto da mensagem sobre correio eletrônico infectado recebido via cc:Mail, na notificação para outros usuários Valor padrão: Nenhum

EMailReport Options

Variável	Descrição
bLogToFile	Tipo: Booleana (1/0) Define se os resultados da varredura devem ser registrados em um arquivo de registro Valor padrão: 1
bLimitSize	Tipo: Booleana (1/0) Define se o tamanho do arquivo de registro deve ser limitado Valor padrão: 1
uMaxKilobytes	Tipo: Número inteiro (10-999) Define o tamanho máximo do arquivo de registro, em quilobytes Valor padrão: 100
bLogDetection	Tipo: Booleana (1/0) Instrui o VShield a registrar os nomes dos vírus detectados Valor padrão: 1
bLogClean	Tipo: Booleana (1/0) Define se os resultados da limpeza devem ser registrados Valor padrão: 1
bLogDelete	Tipo: Booleana (1/0) Define se as operações de exclusão do arquivo infectado devem ser registradas Valor padrão: 1
bLogMove	Tipo: Booleana (1/0) Define se as operações de movimentação do arquivo devem ser registradas Valor padrão: 1
bLogSettings	Tipo: Booleana (1/0) Instrui o VShield a gravar um registro das definições que estão sendo usadas durante a sessão de varredura que precedeu o fechamento do sistema ou o descarregamento do VShield Valor padrão: 1

Variável	Descrição
bLogSummary	Tipo: Booleana (1/0) Instrui o VShield a gravar um resumo de suas descobertas e ações durante a sessão de varredura que precedeu o fechamento do sistema ou o descarregamento do VShield Valor padrão: 1
bLogDateTime	Tipo: Booleana (1/0) Define se a hora e data de um evento devem ser registradas Valor padrão: 1
bLogUserName	Tipo: Booleana (1/0) Define se o nome do usuário deve ser registrado Valor padrão: 1
szLogFileName	Tipo: Seqüência de caracteres Define o nome do arquivo de registro Valor padrão: C:\Program Files\Network Associates\McAfee VirusScan\WebEmail.txt

Módulo Varredura de Download

DownloadGeneralOptions

Variável	Descrição
bEnabled	Tipo: Booleana (1/0) Ativa a varredura dos arquivos obtidos por download Valor padrão: 1
bCanBeDisabled	Tipo: Booleana (1/0) Impede a desativação da varredura dos arquivos obtidos por download Valor padrão: 1

DownloadDetectionOptions

Variável	Descrição
bScanAllFiles	Tipo: Booleana (1/0) Instrui o VShield a examinar todos os arquivos Valor padrão: 0
bScanCompressed	Tipo: Booleana (1/0) Instrui o VShield a incluir os arquivos compactados na varredura Valor padrão: 1
bDetectTrojans	Tipo: Booleana (1/0) Instrui o VShield a examinar vírus do tipo cavalo de Tróia Valor padrão: 1
bDetectJoke	Tipo: Booleana (1/0) Instrui o VShield a examinar vírus do tipo Joke Valor padrão: 1
bDetectCorrupted	Tipo: Booleana (1/0) Instrui o VShield a examinar arquivos danificados Valor padrão: 0
bDetectMaybe	Tipo: Booleana (1/0) Instrui o VShield a examinar as variantes de vírus conhecidos Valor padrão: 1
bProgFileHeuristics	Tipo: Booleana (1/0) Instrui o VShield a examinar arquivos de programas heuristicamente Valor padrão: 0
bMacroHeuristics	Tipo: Booleana (1/0) Instrui o VShield a examinar macros heuristicamente Valor padrão: 0
szProgramExtensions	Tipo: Seqüência de caracteres Define as extensões dos arquivos a serem examinados Valor padrão: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (O ? é um curinga)

DownloadActionOptions

Variável	Descrição
szMoveToFolder	Tipo: Seqüência de caracteres Define a pasta para a qual os arquivos infectados devem ser movidos Valor padrão: \Infectado
szCustomMessage	Tipo: Seqüência de caracteres Define a mensagem personalizada a ser exibida quando um vírus for detectado, se a ação estiver configurada como Solicitar ação Valor padrão: McAfee VShield: Encontrado vírus no arquivo obtido por download!
uScanAction	Tipo: Número inteiro (0/3) Instrui o VShield a realizar a ação especificada quando um vírus é detectado Valor padrão: 0 Valores possíveis: 0 – Solicitar ação 1 – Mover arquivos infectados automaticamente 2 – Excluir arquivos infectados automaticamente 3 - Continuar a varredura
bButtonClean	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário uma opção de limpeza de arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonDelete	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de excluir o arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonExclude	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de eliminar um arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 0

Variável	Descrição
bButtonMove	Tipo: Booleana (1/0) Instrui o VirusScan a fornecer ao usuário a opção de mover o arquivo infectado, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonContinue	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de continuar com o evento interrompido, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonStop	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de negar acesso ao arquivo infectado, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 0

DownloadAlertOptions

Variável	Descrição
bDMIAlert	Tipo: Booleana (1/0) Ativa o Alerta Desktop Management Interface Valor padrão: 0
bNetworkAlert	Tipo: Booleana (1/0) Ativa Alerta Centralizado Valor padrão: 0
szNetworkAlertPath	Tipo: Seqüência de caracteres Especifica uma pasta Alerta Centralizado do servidor Valor padrão: Nenhum
bSoundAlert	Tipo: Booleana (1/0) Ativa um sinal sonoro audível quando um vírus é detectado Valor padrão: 1
bDisplayMessage	Tipo: Booleana (1/0) Define se uma mensagem personalizada deve ser exibida na caixa de diálogo Solicitar ação quando for detectado um controle ActiveX ou miniaplicativo Java hostil, ou uma tentativa de conexão a um URL ou endereço IP banido. Valor padrão: 0

DownloadReportOptions

Variável	Descrição
bLogToFile	Tipo: Booleana (1/0) Define se os resultados da varredura devem ser registrados em um arquivo de registro Valor padrão: 1
bLimitSize	Tipo: Booleana (1/0) Define se o tamanho do arquivo de registro deve ser limitado Valor padrão: 1
uMaxKilobytes	Tipo: Número inteiro (10-999) Define o tamanho máximo do arquivo de registro, em quilobytes Valor padrão: 100
bLogDetection	Tipo: Booleana (1/0) Instrui o VShield a registrar um controle ActiveX ou miniaplicativo Java hostil encontrado, ou uma tentativa de conexão a um URL ou endereço IP banido. Valor padrão: 1
bLogClean	Tipo: Booleana (1/0) Define se os resultados da limpeza devem ser registrados Valor padrão: 1
bLogDelete	Tipo: Booleana (1/0) Define se as operações de exclusão do arquivo infectado devem ser registradas Valor padrão: 1
bLogMove	Tipo: Booleana (1/0) Define se as operações de movimentação do arquivo devem ser registradas Valor padrão: 1
bLogSettings	Tipo: Booleana (1/0) Instrui o VShield a gravar um resumo das definições que estão sendo usadas durante a sessão de varredura que precedeu o fechamento do sistema ou o descarregamento do VShield Valor padrão: 1

Variável	Descrição
bLogSummary	Tipo: Booleana (1/0) Instrui o VShield a gravar um resumo de suas descobertas e ações durante a sessão de varredura que precedeu o fechamento do sistema ou o descarregamento do VShield Valor padrão: 1
bLogDateTime	Tipo: Booleana (1/0) Define se a hora e data de um evento devem ser registradas Valor padrão: 1
bLogUserName	Tipo: Booleana (1/0) Define se o nome do usuário deve ser registrado Valor padrão: 1
szLogFileName	Tipo: Seqüência de caracteres Define o nome do arquivo de registro Valor padrão: C:\Program Files\Network Associates\McAfee VirusScan\WebInet.txt

Módulo Filtro de Internet

INetFltrGeneralOptions

Variável	Descrição
bEnabled	Tipo: Booleana (1/0) Ativa a varredura de arquivos obtidos por download Valor padrão: 1
bCanBeDisabled	Tipo: Booleana (1/0) Impede a desativação da varredura de arquivos obtidos por download Valor padrão: 1

INetFltrDetectionOptions

Variável	Descrição
bScanIP	Tipo: Booleana (1/0) Instrui o VShield a bloquear os endereços IP designados Valor padrão: 1
bScanHost	Tipo: Booleana (1/0) Instrui o VShield a bloquear as URLs designadas Valor padrão: 1
bScanJava	Tipo: Booleana (1/0) Instrui o VShield a examinar miniaplicativos Java potencialmente nocivos Valor padrão: 1
bScanActiveX	Tipo: Booleana (1/0) Instrui o VShield a examinar objetos ActiveX potencialmente nocivos Valor padrão: 1
bDetectTrojans	Tipo: Booleana (1/0) Instrui o VShield a examinar vírus do tipo cavalo de Tróia Valor padrão: 1
bDetectJoke	Tipo: Booleana (1/0) Instrui o VShield a examinar vírus do tipo Joke Valor padrão: 1
bDetectCorrupted	Tipo: Booleana (1/0) Instrui o VShield a examinar arquivos danificados Valor padrão: 0
bDetectMaybe	Tipo: Booleana (1/0) Instrui o VShield a examinar as variantes de vírus conhecidos Valor padrão: 1

Variável	Descrição
bProgFileHeuristics	Tipo: Booleana (1/0) Instrui o VShield a examinar arquivos de programas heuristicamente Valor padrão: 0
bMacroHeuristics	Tipo: Booleana (1/0) Instrui o VShield a examinar macros heuristicamente Valor padrão: 0

INetFltrActionOptions

Variável	Descrição
uScanAction	Tipo: Número inteiro (0/1) Instrui o VShield a atuar da maneira especificada quando uma URL, endereço IP, controle ActiveX ou miniaplicativo Java banido for detectado Valor padrão: 0 Valores possíveis: 0 - Solicitar ação 1 - Negar acesso a objetos

INetFltrAlertOptions

Variável	Descrição
bDMIAlert	Tipo: Booleana (1/0) Ativa o Alerta Desktop Management Interface Valor padrão: 0
bNetworkAlert	Tipo: Booleana (1/0) Ativa Alerta Centralizado Valor padrão: 0
szNetworkAlertPath	Tipo: Seqüência de caracteres Especifica uma pasta Alerta Centralizado do servidor Valor padrão: Nenhum

Variável	Descrição
bDisplayMessage	Tipo: Booleana (1/0) Define se uma mensagem personalizada deve ser exibida na caixa de diálogo Solicitar ação, quando um vírus for detectado Valor padrão: 0
bSoundAlert	Tipo: Booleana (1/0) Ativa um sinal sonoro audível quando uma URL, endereço IP, controle ActiveX ou miniaplicativo Java for detectado Valor padrão: 1
szCustomMessage	Tipo: Seqüência de caracteres Se uma ação for definida como Solicitar ação, esta variável define uma mensagem personalizada que será exibida quando uma URL, endereço IP, controle ActiveX ou miniaplicativo Java banido for detectado Valor padrão: McAfee VShield: Detectado objeto de internet hostil ou site banido!

INetFltrReportOptions

Variável	Descrição
bButtonDeny	Tipo: Booleana (1/0) Instrui o VShield a dar ao usuário a opção de negar acesso ao site no qual o objeto potencialmente perigoso foi detectado Valor padrão: 1
bButtonContinue	Tipo: Booleana (1/0) Instrui o VShield a dar ao usuário a opção de continuar o evento interrompido, se Solicitar ação estiver selecionada e uma URL, endereço IP, controle ActiveX ou miniaplicativo Java banido for detectado Valor padrão: 1
bLogToFile	Tipo: Booleana (1/0) Define se os resultados da varredura devem ser registrados em um arquivo de registro Valor padrão: 1
bLimitSize	Tipo: Booleana (1/0) Define se o tamanho do arquivo de registro deve ser limitado Valor padrão: 1

Variável	Descrição
uMaxKilobytes	Tipo: Número inteiro (10-999) Define o tamanho máximo do arquivo de registro, em quilobytes Valor padrão: 100
bLogDetection	Tipo: Booleana (1/0) Instrui o VShield a registrar os nomes dos vírus detectados Valor padrão: 1
bLogSettings	Tipo: Booleana (1/0) Instrui o VShield a gravar um registro das definições que estão sendo usadas durante a sessão de varredura que precedeu o fechamento do sistema ou o descarregamento do VShield Valor padrão: 1
bLogSummary	Tipo: Booleana (1/0) Instrui o VShield a gravar um resumo de suas descobertas e ações durante a sessão de varredura que precedeu o fechamento do sistema ou o descarregamento do VShield Valor padrão: 1
bLogDateTime	Tipo: Booleana (1/0) Define se a hora e data de um evento devem ser registradas Valor padrão: 1
bLogUserName	Tipo: Booleana (1/0) Define se o nome do usuário deve ser registrado Valor padrão: 1
szLogFileName	Tipo: Seqüência de caracteres Define o nome do arquivo de registro Valor padrão: C:\Program Files\Network Associates\McAfee VirusScan\WebFiltr.txt

Módulo Segurança

SecurityOptions (Opções de segurança)

Variável	Descrição
bPasswordEnabled	Tipo: Booleana (1/0) Define se a proteção por senha será ativada Valor padrão: 0
szPasswordCRC	Reservado. Não modifique
bProtectAllOptions	Tipo: Booleana (1/0) Define se todas as páginas de propriedades serão protegidas por senha Valor padrão: 1
szPasswordProtect	Reservado. Não modifique

Definições Gerais

AVCONFILE

Variável	Descrição
AVCONFILE	Tipo: Seqüência de caracteres Especifica o caminho do AVCONSOLE Padrão: C:\Program Files\Network Associates\McAfee VirusScan\avconsol.ini
SECTION	Tipo: Seqüência de caracteres Especifica o local para relatório no AVCONSOL.INI Padrão: Item_0

Usando as opções da Linha de comando do Virus Scan

Executando a Linha de comando do VirusScan

Você pode executar a Linha de comando do VirusScan em uma janela de prompt do Windows MS-DOS ou reiniciando o computador no modo DOS. A Network Associates recomenda o reinício no modo DOS para obter melhores resultados. Para saber como reiniciar o computador no modo DOS, veja a documentação do Microsoft Windows.

Para executar a Linha de comando do VirusScan, siga estas etapas:

1. Abra uma janela de prompt do MS-DOS no Windows ou reinicie o computador no modo DOS.
2. Vá para o diretório de programas do VirusScan. Se o programa for instalado com as opções padrão, digite esta linha no prompt de comando para localizar o diretório correto:

   ```
   C:\progra~1\networ~1\mcafee~1
   ```

3. Digite `scan`, seguido das opções de varredura que você deseja usar, no prompt de comando.

   A Linha de comando do VirusScan será iniciada imediatamente e começará a examinar o sistema com as opções escolhidas. Ao terminar, exibirá os resultados da operação de varredura, em seguida, retornará ao prompt de comando.

4. Para executar outra operação de varredura, repita a Etapa 3. Para fechar a janela Prompt do MS-DOS, digite `exit` no prompt de comando. Se você reiniciar o computador no modo DOS, digite `win` para iniciar o Windows ou reinicie o computador como você faria normalmente.

As tabelas nas páginas seguintes contêm uma lista de todas as opções do VirusScan disponíveis.

NOTA: Quando você especificar um nome de arquivo como parte de uma opção de linha de comando, deverá incluir o caminho completo do arquivo, se não estiver localizado no diretório de programa do VirusScan.

Opções da linha de comando

Opção da Linha de comando	Limitações	Descrição
Todas as opções relacionadas abaixo podem ser usadas para configurar varreduras por solicitação e ao acessar, a menos que seja estabelecido o contrário.		
/? ou /HELP	Nenhuma.	Há uma lista de opções de linha de comando do VirusScan, cada uma com uma breve descrição.
/ADL	Somente a opção de varredura por solicitação.	Examinar todas as unidades locais — inclusive as unidades compactadas e as placas de PC, mas não os discos — além de todas as outras unidades especificadas na linha de comando. Para examinar as unidades locais e de rede, use os comandos /ADL e /ADN juntos na mesma linha de comando. OS/2: /ADL inclui a unidade de CD-ROM na varredura, quando utilizado com /NODDA.
/ADN	Somente a opção de varredura por solicitação.	Examina todas as unidades de rede — inclusive a unidade de CD-ROM — para procurar vírus, além de quaisquer outras unidades especificadas na linha de comando. *Nota:* Para examinar as unidades local e de rede, use os comandos /ADL e /ADN juntos na mesma linha de comando.
/ALERTPATH *<dir>*	Somente a opção de varredura por solicitação.	Designa o diretório *<dir>* como um caminho de rede monitorado pelo Alerta Centralizado.
/ALL	Somente a opção de varredura por solicitação.	Anula a configuração padrão pela varredura de todos os arquivos infectáveis — independentemente da extensão. *Notas:* O uso da opção /ALL aumenta substancialmente o tempo de varredura necessário. Utilize-a se você encontrar um vírus ou suspeitar que há algum. Como padrão, o VirusScan examina apenas os arquivos com as seguintes extensões: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF e .VXD. Estes são os arquivos mais suscetíveis a vírus.

Opção da Linha de comando	Limitações	Descrição
/ANALYZE	Somente a opção de varredura por solicitação. É necessária memória estendida.	Define o VirusScan para um exame que utiliza a heurística completa, de programa e macro. *Nota:* /MANALYZE busca vírus de macro apenas; /PANALYZE procura somente vírus de programa.
/ANYACCESS	Somente a opção de varredura ao acessar.	Examina: * o setor de inicialização sempre que o disco for lido ou gravado * executáveis * qualquer arquivo novo criado.
/APPEND	Somente a opção de varredura por solicitação.	Usada com /REPORT para anexar o texto da mensagem de relatório ao arquivo de relatório especificado, em vez de substituí-lo.
/BOOT	Somente a opção de varredura por solicitação.	Examinar somente o setor de inicialização e o registro de inicialização.
/BOOTACCESS	Somente a opção de varredura ao acessar.	Examina o setor de inicialização de um disco para buscar vírus quando for acessado (inclusive nas operações de leitura/gravação).
/CLEAN	Somente a opção de varredura por solicitação.	Limpa os vírus de todos os arquivos infectados e das áreas do sistema.
/CLEANDOCALL	Somente a opção de varredura por solicitação.	Como medida de precaução contra os vírus de macros, o /CLEANDOCALL limpa todas as macros dos documentos do Microsoft Word e Office. *Nota:* Esta opção exclui todas as macros, inclusive as que não estão infectadas por vírus.
/CONTACT *<mensagem>*	Somente a opção de varredura ao acessar.	Exibe uma mensagem especificada quando um vírus é detectado. Esta mensagem deve conter até 255 caracteres.

Opção da Linha de comando	Limitações	Descrição
/CONTACTFILE *<nome do arquivo>*	Nenhuma.	Exibe o conteúdo do *<nome do arquivo>* quando um vírus é encontrado. Esta é uma oportunidade para fornecer informações sobre contato e instruções para o usuário, quando um vírus for encontrado. Esta opção é útil principalmente em ambientes de rede, pois você pode facilmente manter o texto da mensagem em um arquivo central, sem precisar colocá-la em cada estação de trabalho. *Nota:* Qualquer caractere é válido em uma mensagem de contato, exceto a barra inclinada para a esquerda (\). As mensagens iniciadas por uma barra diagonal (/) ou um hífen (-) devem ser colocadas entre aspas.
/DEL	Somente a opção de varredura por solicitação.	Exclui os arquivos infectados permanentemente.
/EXCLUDE *<nome do arquivo>*	Somente a opção de varredura por solicitação.	Não examina ou adiciona códigos de validação aos arquivos relacionados em *<nome do arquivo>*. Use esta opção para: * Excluir arquivos específicos de uma varredura. Mostra o caminho completo de cada arquivo que você deseja excluir em linhas separadas. Você pode usar coringas * e ?
/FILEACCESS	Somente a opção de varredura ao acessar.	Examina os arquivos executáveis quando são acessados e também durante a execução. *Nota:* Esta varredura *não* verifica o setor de inicialização.
/FREQUENCY <*n* >	Somente a opção de varredura por solicitação.	Não faz a varredura <*n*> horas após o exame anterior. Nos ambientes onde o risco de infecção viral é muito baixo, use esta opção para evitar varreduras desnecessárias. Lembre-se de que, quanto maior a freqüência de varreduras, maior a proteção contra infecções.
/HELP ou /?	Nenhuma.	Há uma lista de opções de linha de comando do VirusScan, cada uma com uma breve descrição.
/IGNORE *<unidade(s) de disco>*	Somente a opção de varredura ao acessar.	Não verifica os arquivos carregados a partir da(s) unidade(s) de disco especificadas.

Opção da Linha de comando	Limitações	Descrição
/LOAD *<nome do arquivo>*	Somente a opção de varredura por solicitação.	Carregar as opções de varredura a partir do arquivo nomeado. Use esta opção para executar uma varredura que você já tenha configurado ao carregar as definições padrão salvadas em um arquivo no formato ASCII.
/LOCK	Não está disponível em ambientes com memória baixa.	Com esta opção /LOCK ativada, o VirusScan interromperá a operação e bloqueará o sistema, se encontrar um vírus. A opção /LOCK é adequada para ambientes de rede altamente vulneráveis, como laboratórios de informática de uso aberto. A Network Associates recomenda o uso da opção /LOCK com /CONTACTFILE para informar aos usuários o que devem fazer ou quem contatar se o VirusScan bloquear o sistema.
/MANALYZE	Somente a opção de varredura por solicitação. É necessária memória estendida.	Define os recursos de varredura heurística do VirusScan para examinar somente vírus de macro. *Nota:* O /PANALYZE procura somente vírus de programa; /ANALYZE procura vírus de macro e de programa.
/MANY	Somente a opção de varredura por solicitação.	Examina diversos discos consecutivamente em uma unidade de disco. O VirusScan lhe pedirá cada disco. Use esta opção para verificar diversos disquetes rapidamente. Você não pode usar a opção /MANY se estiver executando o VirusScan a partir de um disco de inicialização e tiver apenas uma unidade de disquete.
/MAXFILESIZE *<xxx.x>*	Somente a opção de varredura por solicitação.	Examina apenas os arquivos que tenham menos de *<xxx.x>* megabytes.
/MEMEXCL		Exclui o endereço de memória A0000:0000 da varredura.

Opção da Linha de comando	Limitações	Descrição
/MOVE *<dir>* ou *.???	Somente a opção de varredura por solicitação.	*/MOVE <diretório>:* Move todos os arquivos infectados encontrados durante uma varredura para o diretório especificado, preservando a letra da unidade de disco e a estrutura do diretório. *Nota:* Esta opção não tem efeito se o Registro de inicialização principal ou o setor de inicialização estiver infectado, pois estes não são arquivos de fato. */MOVE*.???:* O VirusScan irá alterar a extensão dos arquivos infectados, mas não os moverá. Por exemplo, o uso da opção /MOVE*.BAD resultará na renomeação dos arquivos infectados com a extensão .BAD, mas não serão movidos fisicamente.
/NOBEEP	Somente a opção de varredura por solicitação.	Desativa o alerta audível emitido cada vez que o VirusScan encontra um vírus.
/NOBREAK	Somente a opção de varredura por solicitação.	Desativa CTRL-C e CTRL-BREAK durante as varreduras. Os usuários não poderão interromper as varreduras em andamento se for utilizado o /NOBREAK.
/NOCOMP	Somente a opção de varredura por solicitação. É necessário memória estendida.	Ignora a verificação dos executáveis compactados criados com os programas de compactação LZEXE ou PkLite. Isto reduz o tempo de varredura quando um exame completo não é necessário. Caso contrário, como padrão, o VirusScan verifica o conteúdo dos arquivos auto descompactáveis ou executáveis descompactando-os na memória e verificando as assinaturas de vírus. VirusScan examinará as modificações nos executáveis compactados, se eles contiverem os códigos de validação do VirusScan.

Opção da Linha de comando	Limitações	Descrição
/NODDA	Somente a opção de varredura por solicitação.	Sem acesso direto a disco. Esta opção impede o VirusScan de acessar o registro de inicialização. Este recurso foi adicionado para permitir que o VirusScan seja executado no Windows NT. Você pode precisar usar esta opção em algumas unidades orientadas por dispositivos. A A utilização de /NODDA com /ADN ou /ADL pode gerar erros ao acessar unidades de CD-ROM ou unidades Zip vazias. Se isso acontecer, digite F (para Falhar) como resposta às mensagens de erro, a fim de continuar a varredura.
/NODISK	Somente a opção de varredura ao acessar.	Não examina o setor de inicialização ao carregar o VShield.
/NODOC	Somente a opção de varredura por solicitação.	Não examina os arquivos do Microsoft Office.
/NOEMS	Somente a opção de varredura ao acessar.	Impede que o VShield use a memória estendida (EMS).
/NOEXPIRE	Somente a opção de varredura por solicitação.	Desativa a mensagem “data de validade” caso os arquivos de dados do VirusScan estejam vencidos.
/NOMEM	Nenhuma.	Não examina a memória em busca de vírus. Reduz sensivelmente o tempo de varredura. Use a opção /NOMEM apenas quando estiver absolutamente seguro de que o seu computador não contém vírus.
/NOREMOVE	Somente a opção de varredura ao acessar.	Impede que o VShield seja removido da memória com a chave /REMOVE.
/NOWARMBOOT	Somente a opção de varredura ao acessar.	Não examina o setor de inicialização da unidade de disquete A: durante a inicialização à quente (reinicialização do sistema ou CTRL+ALT+DEL).

Opção da Linha de comando	Limitações	Descrição
/NOXMS	Somente a opção de varredura ao acessar.	Não usa a memória estendida (XMS).
/ONLY *<unidade(s)>*	Somente a opção de varredura ao acessar.	Examina somente arquivos carregados de unidade(s) especificada(s).
/PANALYZE	Somente a opção de varredura por solicitação. É necessária memória estendida.	Configura o VirusScan para examinar usando heurística de programa. *Nota:* /MANALYZE procura somente vírus de macro; /ANALYZE procura vírus de programa e de macro.
/PAUSE	Somente a opção de varredura por solicitação.	Ativa a pausa de tela. O prompt “Pressione qualquer tecla para continuar” aparecerá quando o VirusScan preencher uma tela com mensagens. Caso contrário, como padrão, o VirusScan preenche e rola uma tela continuamente, sem parar, o que permite que o VirusScan seja executado em PCs com múltiplas unidades ou que tenham graves infecções, sem necessitar de interferências. A Network Associates recomenda a omissão de /PAUSE ao usar as opções de relatório (/REPORT, /RPTCOR e /RPTERR).
/PLAD	Somente a opção de varredura por solicitação.	Preserva as datas do último acesso em unidades Novell NetWare. Normalmente, essas unidades de rede atualizam a última data de acesso Quando o VirusScan abre e examina um arquivo. Entretanto, alguns sistemas de backup em fita usam esta última data de acesso para decidir se devem fazer um backup do arquivo. Use a opção /PLAD para assegurar que a última data de acesso não será alterada como resultado da varredura.
/RECONNECT	Somente a opção de varredura ao acessar.	Restaura o VShield depois de ter sido desativado por certos controladores ou programas residentes na memória.

Opção da Linha de comando	Limitações	Descrição
/REMOVE	Somente a opção de varredura ao acessar.	Descarrega o VShield da memória.
/REPORT *<filename>*	Somente a opção de varredura por solicitação.	Cria um relatório de arquivos infectados e erros de sistema, e salva os dados em *<nome do arquivo>* em formato de arquivo de texto ASCII. Se o *<nome do arquivo>* já existir, /REPORT irá substitui-lo. Para evitar a substituição do arquivo, use a opção /APPEND com /REPORT: isto fará com que o VirusScan anexe as informações do relatório no final do arquivo, em vez de sobregravá-lo. Você pode também usar /RPTALL, /RPTCOR e /RPTERR para adicionar arquivos examinados, arquivos danificados, arquivos modificados e erros de sistema no relatório. Pode ser incluída a unidade e o diretório de destino (como D:\VSREPRT\ALL.TXT), mas se a unidade de destino for de rede, você deverá ter direitos para criar e excluir arquivos naquela unidade. A Network Associates recomenda a omissão de /PAUSE ao utilizar qualquer opção de relatório.
/RPTALL	Somente a opção de varredura por solicitação.	Inclui todos os arquivos examinados no arquivo /REPORT. Quando usada com /REPORT, esta opção adiciona os nomes dos arquivos danificados ao arquivo de relatório. Você pode usar /RPTCOR com /RPTERR na mesma linha de comandos. A Network Associates recomenda a omissão de /PAUSE ao usar qualquer opção de relatório.

Opção da Linha de comando	Limitações	Descrição
/RPTCOR	Somente a opção de varredura por solicitação.	Inclui os arquivos danificados no arquivo /REPORT. Quando usada com /REPORT, esta opção adiciona os nomes de arquivos danificados ao arquivos de relatório. Os arquivos danificados encontrados pelo VirusScan podem ter sido danificados por um vírus. Você pode usar /RPTCOR e /RPTERR na mesma linha de comandos. Podem ocorrer leituras falsas em alguns arquivos que requerem um arquivo de sobreposição ou outro executável para funcionarem corretamente (ou seja, arquivos que não são autoexecutáveis). A Network Associates recomenda a omissão de /PAUSE ao usar qualquer opção de relatório.
/RPTERR	Somente a opção de varredura por solicitação.	Inclui erros no arquivo /REPORT. Quando usada com /REPORT, esta opção adiciona uma lista de erros de sistema ao arquivo de relatórios. A opção /LOCK é adequada para ambientes de rede altamente vulneráveis, como laboratórios de informática de uso aberto. Você pode usar /RPTERR com /RPTCOR na mesma linha de comandos. Erros de sistema podem incluir problemas de leitura ou gravação em um disco ou disco rígido, problemas no sistema de arquivos ou na rede e outros problemas relacionados ao sistema. A Network Associates recomenda a omissão de /PAUSE ao usar qualquer opção de relatório.
/SAVE	Somente a opção de varredura ao acessar.	Salva as opções da linha de comando no arquivo VSHIELD.INI.
/SUB	Somente a opção de varredura por solicitação.	Examina os subdiretórios em um diretório. Como padrão, quando você especifica um diretório para ser examinado em vez de uma unidade, o VirusScan examinará somente os arquivos nele contidos e não seus subdiretórios. Use /SUB para examinar todos os subdiretórios em qualquer diretório especificado. Não é necessário usar /SUB se você estiver examinando uma unidade inteira.

Opção da Linha de comando	Limitações	Descrição
/UNZIP	Somente a opção de varredura por solicitação. É necessário memória estendida.	Examina o conteúdo dos arquivos compactados.
/VIRLIST	Somente a opção de varredura por solicitação.	Exibe o nome e uma breve descrição de cada vírus detectado pelo VirusScan. Você pode usar a opção /PAUSE na mesma linha de comando que /VIRLIST para ler cada tela da lista de vírus. *Para redirecionar a saída de /VIRLIST para um arquivo de texto:* No aviso do comando, digite: scan /VIRLIST> nome do arquivo.txt Como o VirusScan pode detectar muitos vírus, esse arquivo terá mais de 250 páginas. Ele é muito grande para que o programa “Editar” do MS-DOS o abra; a Network Associates recomenda o uso do Bloco de Notas ou de outro editor de texto para abrir a lista de vírus.
/XMSDATA	Somente a opção de varredura ao acessar.	Carrega os arquivos de dados do VShield na memória XMS.

Índice

Symbols

A

D

E

F

H

I

L

M

P

Q

T

U

V

W

Z